Developments in process control computer systems (1973-1978)

Taylor, J.R.; Goodstein, L.P.

Publication date:
1973

Document Version
Publisher's PDF, also known as Version of record

Risö-M-1591

Risö-M-1591

Danish Atomic Energy Commission

Research Establishment Risö

ELECTRONICS DEPARTMENT

Developments in

Process Control Computer Systems

(1973-1978)

by

J.R. Taylor and L.P. Goodstein

March 1973

R-5-73

Available on request from: Library of the Danish Atomic Energy Commission
(Atomenergikommissionens Bibliotek), Risö, DK-4000 Roskilde, Denmark.
Telephone: (03) 355101, telex: 5072

A. E. K. RISØ

RISØ - M -

RISØ - M -

Title and author(s)

Date

Department or group

Group's own registration number(s)

pages + tables + illustrations

Abstract

Copies to

Abstract to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, Roskilde, Denmark.
Telephone: (03) 35 51 01, ext. 334, telex: 5072.

FI 25-204

Table of Contents

ISBN 87 550 0188 2

Section 1

THE SITUATION TODAY

A brief review of the situation regarding the use of process computers as it stands today will be presented. It can serve as a reference framework against which some ideas about future developments to be given later can be viewed, compared and evaluated. The applications which are of direct interest here lie in the areas of conventional and nuclear power generation, although one should not omit completely mention of the use of computers for the monitoring and control of power distribution (1,2).

The inclusion of a digital computer in conventional power plants dates back to the time of LITTLE GYPSY I and Etiwanda 3 and 4 (1961-3) in the US after power plant automation studies carried out by the respective companies indicated that the use of a digital computer would be advantageous for the automatic supervision of the plant. These first attempts were not complete successes but, in the following years, technological developments in the computer field coupled with a more careful choice of application have led to a steadily increasing acceptance of the use of digital computers. For example, statistics from a recent American survey (3) indicate that of 42 conventional power stations

79% had automatic data collection
69% had performance computers
31% had some form for computer control.

In time, the economic factor will completely justify the wider use of computers; at the moment, questions regarding reliability remain.

The review will be restricted to the situation in the UK and Canada since the utilization of computers in power plants has to some extent been the most advanced in these two countries. However, reference should also be made to work being carried out in Germany and Norway (4,5).

The UK

Jervis, in an informative survey article (6), explains the English (CEGB) point of view regarding the use of computers in

both conventional and nuclear plants. The trend toward centralized monitoring and control has made the use of computers attractive for the display and recording of data and alarms, especially if a savings in operating staff can be achieved at the same time. With regard to conventional plants, an economic case for computer control has not been established, however, since the average replacement cost of generating capacity for these stations coupled with their fairly short (hot) start-up times give cost penalties over the life of the station which are low compared to the cost of a comprehensive computer control system. Therefore, most English thermal stations are capable of operating indefinitely without the computer with the only restriction imposed by its unavailability being the loss of some start-up functions and detailed monitoring and logging.

On the other hand, nuclear power stations give a considerably higher cost penalty for outages and therefore a suitably reliable (= redundant) computer control system (without extensive back-up) which keeps outage rates down can be economically justified.

Table 1 from Jervis' article summarizes the tasks assigned to the computers in the various stations.

The following comments regarding these tasks may be relevant:

a) CEGB does not consider the use of the computer in a non-redundant configuration as acceptable for auxiliary system sequence control. Since conventional plant is provided normally with single computer systems, wired program sequence control equipment is used.

b) Turbogenerator startup and loading via the computer is quite common.

c) CEGB prefers DDC for economical reasons in the new nuclear stations and is planning extensive use of this in Hartlepool, for example.

d) CEGB does not perform off-line calculations or other tasks on an on-line computer; in fact, they consider any on-line modification and development of programs to be extremely hazardous and therefore do not provide any facilities for doing this.

TABLE 1

MAIN COMPUTER-SYSTEM FACILITIES IN CEGB POWER STATIONS

	Nuclear stations							Coal/oil stations						
								Fawley						
	Early nuclear stations	Oldbury	Wylfa	Dungeness B	Hinkley Point B	Hartlepool	Bradwell	Kingsnorth	Main system	Auxiliary boiler	Pembroke	Desk	Wall	Grids
Board-scan-detection logging	Some	•	•	•	•	•								
Plant-sensing control and recording				•										
Performance logging and alarm	All	•	•	•	•	•	•	•	•	•	•	•	•	•
C.R.T. data display												•		
Alarm analysis		•						•		•				
Alarm display												•		
Logging														
Routine logging		•	•	•	•	•	•	•	•	•	•	•		
Postincident logging														
Startup control:														
Boiler startup				•		•								
Startup pressure control									•			•		
Boiler-analogue-controller										•				
Water treatment			•		•			•	•			•		
Turbine ramp														
Turbine loading						•								
Load-changing governor														
Boiler-feed-pump pump				•		•								
Steady-points control														
Reactor coolant outlet temperature				•		•	•							
Reactor coolant inlet temperature							•							
Reactor coolant mass flow														
Feed flow														
Steam pressure														
Steam temperature														
Air-fuel ratio														
Drum level														
Gas temperature														
Component regulator position														
Feed-oil temperature														
Main steam temperature														
Other														
Performance calculations												•		
Offline calculations														
Nonessential on-line logging faults		•	•	•	•	•			•	•	•			
Modification of logging (selected data)					•							•		

TABLE 2

PLANT ITEMS AND COMPUTER-SYSTEM DETAILS FOR CEGB POWER STATIONS

Coal-fired stations

Nuclear stations

	Oldbury	Wylfa	Dungeness B	Hinkley B	Hartlepool (1) Heysham (1)	Bradwell	Hunterston	Kingsnorth	Main system	Auxiliary boiler	Fendrake	Drax	Isle of Grain
Plant items:													
Plant	Magnox	Magnox	Mark II AGR	Mark II AGR	Mark II AGR (1) 1969 74 (2) 1971 76	Magnox Replacement system	Coal-fired 1967 73	Coal-fired 1967 73	Oil	Oil	Oil	Oil 1944 72	Oil 1971 75
Years of start on site to completion													
Status of computer system	Operating	Operating	Commissioning	Works test	Site test	Commissioning	Operating	Operating	Experimental	Operating	Commissioning	Manufacture
Number and make of computers per site, NW	1 × 332	4 × 335	2 × 860	2 × 860	4 × 52	4 × 360	4 × 320		4 × 500		2 × 360		
Basic cycle time, μs	4	4	1.8	1.8	1.8								
Gas circulators per reactor	4	4	4	4	4								
Main channels per reactor	3301	6156	812	360	324	1600							
Fuel channels per reactor	331	195	69	44	81	119							
Computer-system details													
Core-store system:													
Number and make of processors per site		2 × 2484	2 × 2048	2 × 2400	3 × 3500	380 - 684	920	4 × 1200	37	4 × 1024 - 128	2304	5 × 512
Maximum rate per processor (words per second)	Separate figure	150	128	195	128	Random 155 (maximum)	200	190	32		200 (maximum)	Random 250 (maximum)
Digital input channels:													
Maximum, here, all process input channels	3000	2 × 1920	2 × 3750	2 × 2048	2 × 2048		1800	4 × 1000	56	4 × 288 + 448	9048	5 × 1128
Maximum rate, all process input channels	0.25	0.25	0.25	0.1	0.25			0.125		0.28	40 ms	Random 0.25
Main-store system:											320 ms	
Number and make of processors per site												
Main-store capacity (words per processor)												
Number of banks (for interleaving)		4	10	74	74		4				5	5
Number of ways			2	2	2							
Remote starting			2	2	2							
Others			b.d.d.		As Table 1				As Table 1				
Secondary-storage unit:													
Number of drives		2	3	2	3	1	1	4	1	1	1	5
Manufacturer	AEI	EMI	Ferranti	EE Co.	Ferranti	Honeywell	Honeywell	EE Co.	Elliott	Elliott	EE Co.	EE Co.	Honeywell
Model	4690	2.C	Argus 500	16-45-40	Argus 500	H316	H316	4077	4130	4130	16-45-40	16-45-40	316
Word length, bits	44	20	24	16	24	18	18	24	32	32	16	16	16
Working store capacity, words													
Number of bits	4	10	24	48	24	12	4	18	6	56	48	48
Working store cycle time, μs	8.5	2	2	1	2	1.4	4	2	Diverse	Integrated	Integrated	Integrated
Organization	Diverse	Diverse	Diverse	Integrated	Integrated	Integrated	Diverse	Diverse	Diverse	Diverse	Integrated	Integrated	Integrated
Peripheral-store words	On	On	On	Multilayer	Multilayer	Multilayer	On	On	On	On	Multilayer	Multilayer	Multilayer
Auxiliary store:	Open	Open	Open				Open	Open	Open	Open			
Type	Drums	Drums	Drums	Drums	Discs	Disc	Drum	Drums			Drums	Drums	Discs
Capacity (total including redundancy), k words	2 × 8	3 × 64	4 × 315	4 × 600	4 × 600	1 × 60	1 × 60	4 × 256			3 × 300	1 × 300	5 × 300
Channels:													
Number of channels, site	AEI	Marconi	Ferranti	Marconi	Ferranti	Cossor	Elliott	Marconi		Marconi	Marconi	Marconi	Cossor
Rate of data channel, max	330	330	330	420	330	375	375	330 525		480	480 330	480 330	375
Number of bits in word	24	24	24	24	24	24	24			24	24	24	18 (Modular)
Number of bits in unit										2 × 9 + 1 spare	10 + 8		
Number of tubes in	2 × 2	2 × 5	2 × 8	2 × 5	2	3 × 4	4 + 1 spare		4 × 4	2 × 5			
Input-unit data													
Number of tubes in common	2	4	(20 outlets total)		1						1		
Number of tubes in vertical		2	2	2					2	2			
Power		6											
Total	14.15	14.21	17	19	8	8	7	16 + 1 spare	56	8	8	4	
System configuration in Fig. 2	b	c	d	d	a	a	f	b, d, d, f					

The figures are approximate and are per station, unless otherwise stated

Dual nuclear station has two reactors

e) CEGB is a pioneer in the area of "alarm analysis". Beginning with Oldbury and Wylfa, they have used the computer to analyze strings of related alarms and give the operator information on the primary cause together with a suggestion for action. In this survey article, Jervis makes the point that the price for alarm analysis software is very high and that CEGB plans to reduce its complexity in future stations. It is perhaps significant to note that the Isle of Grain plant, the newest of the conventional stations, will not have alarm analysis.

Table 2 gives further details on the computer systems employed and includes references to an appropriate configuration sketch on Fig. 1.

It is seen that conventional plants have computer configurations which either consist of a single computer system shared among all plant units or a separate computer system per plant unit. More computer control functions are acceptable in plants with the latter organization and in one of these newer stations (Isle of Grain), CEGB is actually using mini-computers with an expanded working store and backing disc. In addition, an extra computer for common services is included. In other plants, a computer type with a separate "arithmetic and logic processor" and up to 14 separate "input/output processors" which all share main store is employed.

CEGB has apparently not yet been able to standardize on a configuration for their conventional stations. The computer/plant item permits development, testing and commissioning to occur individually as required while a common computer can offer some economy due to resource sharing.

In all but the earliest MAGNOX nuclear plants, some form for redundancy is provided. Since all of these stations consist of reactor/turbine/generator pairs, the standby capacity is shared between the two units. Fig. 1 b-d illustrate the various forms for redundancy which are used. These are all "external" in the sense that complete cpu-store-local peripheral sub-systems are replaced when a computer switch-over takes place. These systems have well-defined change-over points which can be suitably designed for high reliability. A typical example is shown in Fig. 2.

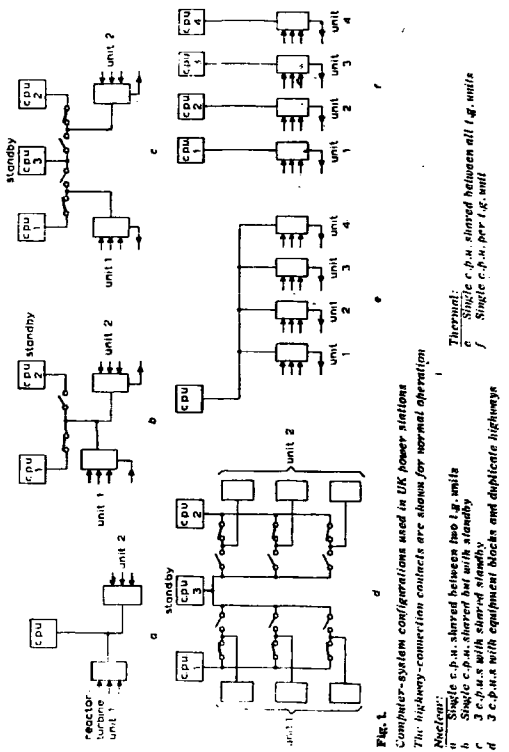


Fig. 1
Computer-system configurations used in UK power stations
The highway-connection contacts are shown for normal operation

Nuclear:
a Single c.p.u. shared between two l.g. units
b Single c.p.u. shared but with standby
c 3 c.p.u.s with shared standby
d 3 c.p.u.s with equipment blocks and duplicate highways

Thermal:
e Single c.p.u. shared between all l.g. units
f Single c.p.u. per l.g. unit

CEGB has established criteria for the reliability of the computer-power station combination. Fault behavior is classified into the following four states: (quoted from Jervis)

"State 0: The system is completely operational and without any module faults. All standby equipment is operational in this state.

State 1: The system is operational so that it does not place any restrictions on the control of the reactor-turbine unit. State 1 is normally required for the startup of the reactor or turbine. It should be noted that, for state 1, some modules may have failed, i.e. the standby may be in use.

State 2:Faults have occurred so that the control of the reactor turbine unit is severely restricted. Such restrictions on control probably amount to operation at steady load. The actual facilities required to be operational in state 2 have a major effect on the configuration of the computer system.

State 3: More faults have occurred so that the computer system cannot be used for operating the plant. If conventional backup control and instrumentation were not provided, the reactor-turbine unit would have to be shut down.

The following is an example of some considerations relating to the various states that apply to a CEGB mark II reactor system having full d.d.c. with sufficient backup equipment to operate in state 3 at steady load for at least 10 min.

State 0: The design target is a system with an availability of at least 99.5% over a system life of 30 years, i.e. total downtime of less than 44 h per year.

State 1: The design target for this state is an availability of 99.9%. For a nuclear station being started up 100 times in its station life, the probability of computer failure preventing a startup should be 0.1.

State 2: No single fault on a reactor-unit computer system should cause a change from state 0 to state 2. For the configuration of Fig.2 the minimum facilities for the mainten-

ance of state 2 are indicated in Table 3. These correspond to the loss of a single equipment block defined in Fig. 2.

State 3: The probability of a reactor-unit computer system failing to state 3 should be lower than 0.5 for once in 7 years. The corresponding figure for the 2-reactor computer system should be once in 30 years. The degradation from state 0 to state 3 will be due to the combination of several failures. The maximum reinstatement time of the system from state 3 to state 0 should be less than 4 h."

The following guidelines were used in arriving at the contents of each "block" shown in Table 3 and Fig. 2.

(a) Where an item of equipment is time-shared, and the loss of all facilities would result from its failure, a standby is provided with automatic changeover. Examples are the central processor units, the auxiliary stores and the main-power-supply motor-generator sets.

(b) Where it is uneconomical to provide 100% redundancy, diversity is employed to restrict the consequences of the failure, e.g. by splitting the inputs into relatively small blocks of, say, 500 analogue inputs per scanner.

(c) Where the failure of a peripheral can block the highway, automatic isolation arrangements are provided to disconnect the faulty unit.

(d) Adequate peak loading capacity is provided so that an acceptable, but reduced, service is available at non-peak times although one part may be out of action. An example of this is the c.r.t. system, which is divided into two parts, either of which is normally adequate for running the reactor for a few hours.

(e) Where certain information is vital, it is fed through two channels, so that a single failure does not cause its loss, though it may reduce the scanning speed.

(f) The electronic components used have a generous rating in terms of the temperature environment in which the equipment operates. The printers are normally allocated to specific duties, and are lightly loaded to extend their life.

Items (b), (d) and (e) are examples of graceful degradation.

(g) Facilities are provided to test the peripherals on a c.p.u. In nuclear stations, this is usually done offline, so as not to interfere with normal operation, and special diagnostic software is provided.

Table 3

Example of the allocation of facilities and the fraction lost by equipment-block failure

Equipment block	Component of block	Overlap or duplication	Fraction of facility lost by failure of equipment block
1	C.R.T.		1/3
	Disc	Duplicated	0
2	Analogue inputs	90% overlap	1/10
	Digital inputs	Duplicated	0
	1/3 digital outputs		1/3
	1 printer		1/4
	1 punch		1
3	Analogue inputs	90% overlap	1/10
	C.R.T.		1/3
	Digital inputs	Duplicated	0
	1/3 digital outputs		1/3
	2 printers		1/2
4	C.R.T.		1/3
	Disc	Duplicated	0
	Digital inputs	Duplicated	0
	1/3 digital outputs		1/3
	1 printer		1/4
	1 tape reader		1

Note that the blocks are shown in Fig. 2.

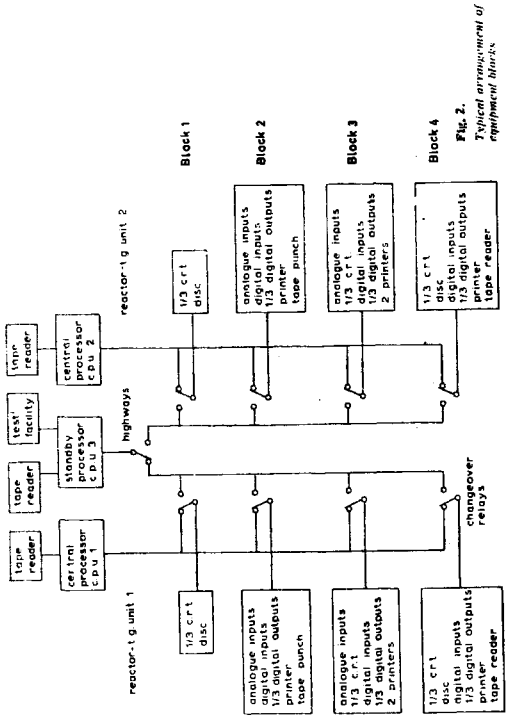


Fig. 2. *Typical arrangement of equipment blocks*

In the newest nuclear stations (Hartlepool and Heysham) (8, 9), the input scanning equipment for both contact and analog inputs is located in remote areas to save on cable costs. Five separate groups of 512 analog and up to 506 contact inputs are used, each in areas where the signals to be monitored are generated. This division gives a further saving on high premium floor area in the region of the central control room with a reduction in ventilation requirements.

Jervis, in another paper (7), gives some reported availability figures for European nuclear power plants. His data are reproduced in Table 4 and, although subject to the usual difficulties in interpretation of such information coming from different sources, they indicate that present-day redundant computer-based instrumentation systems have an availability of 99.8% or better over a 1/2 to 1 year operating interval.

Table 4

Some reported availability figures for nuclear power plants

Station	System	Year & period	% Availability	Remarks
A	1 cpu serving 2 reactors	1970/71 1 year	95.3	
B	1 cpu & standby serving 2 reactors	1970/71 1 year	99.88	
C	1 cpu serving one reactor with shared standby	1971 6 months	99.94	Special site test with limited programs Continuous maintenance attendance
D	1 cpu serving one reactor	1971 9 months	98.54	
E	"	1969 1970 1971	95 95.9 98.7	Computer used for on-line and off-line operation
F	"	1971	99.75	Experimental plant
G	"	1971	98-99	

Canada

Canadian applications of computers in their nuclear stations can also be of interest (10,11). Their reactors are all heavy water moderated with natural uranium and either light or heavy water cooling. The newer reactors are large enough in physical size to require multi-dimensional control features.

Douglas Point was the first station with some form for computer control. It employs a single machine which is used, among other things, for set-point control on fast power regulation and DDC to counter any flux tilt in the core. However, the reactor can operate without the computer. The Douglas Point installation is somewhat unique in that there exists a physical connection between the computer and the independent safety system. "AND" circuits in the safety system receive one input from the computer. These signals monitor the outlet temperature in each group of fuel channels. The other input (flow) is processed independently. If flow is low and temperature is high in the same group of channels, the reactor will be tripped. The computer also monitors some of the safety sensors to permit better testing for rationality.

Three later stations, Pickering, Gentilly and Kanupp, all use double computer systems (see Table 5) which perform DDC or set-point control in various critical loops. Cost factors mitigated against a three computer arrangement and reliability factors ruled out the use of a single computer. Analog or manual backup was not considered to be feasible.

In Pickering, xenon-induced instability has lead to dynamic control of reactivity by the computer in zones where the light water level can be controlled in each of 14 zones - either independently or in unison. In addition, the computer system controls boiler pressure, computes plant power set-point, controls the fuelling machine and monitors several hundred plant variables.

Vital control tasks are executed by each computer using the same set of triplicated input signals but only one machine is connected to the actual controller if a "standby" mode is employed. If a failure occurs in the controlling computer, a changeover unit switches the controller to the other computer. If the second computer fails, control reverts to one of several

Table 5

Canadian control computer configurations

	Douglas Point	Pickering	Gentilly	Kanupp	Bruce (17)
Rating (e)	1 x 200 MW	4 x 500 MW	1 x 250 MW	1 x 137 MW	4 x 750 MW
Computer/block	(1)CDC 636	(2)IBM 1800	(2)SEL 810A	(2)GEPAC 4020	(2)VARIAN 620f
Per computer					
Core store	8 K x 15 bits	16 K x 16 bits	16 K x 16 bits	8 K x 24 bits	32 K x 16 bits
Backing store	50 K drum	132 K drum	228 K disc	53 K drum	262 K disc fixed 585 K disc moving
Analog inputs	550	860/block	512	400	1000-1500
Scan rate	1000/sec	10,000/sec	10,000/sec max	5000/sec	-
Digital inputs	80	1000/560	370	380/840	512
Analog outputs	17	42	30 total	10	32
Digital outputs	46	512	608 total	33	384
Availability	99.4% '64-'66 99.2% '67				

fail-safe conditions. In addition, each computer monitors sets of critical parameters (such as channel outlet temperature) and, if both agree that a temperature is too high, a special action such as controlled power set-back will take place. Other less vital tasks such as control of the fuelling machine or process monitoring are split between the two computers.

In Gentilly (12), the computer system performs DDC of booster rods for coarse reactivity control, of absorber rods for power control and spacial control (via stepping motors) and of coolant flow as a function of power. Input signals for essential functions are connected to both computers. However, the control program will normally run only in one machine. A detected failure in the active machine will result in a signal to the other to take over control. If both machines fail, the reactor will be shut down.

A CRT display is included for the presentation of messages, trend curves and power distribution plots.

Kanupp in Pakistan uses DDC extensively for control of power and reactivity. Here, a "parallel" form for control is used. The instrumentation system is dual from sensors to controllers. Moderator level control is exercised by both computers with each controlling one of the two valves. In practice, one computer has its set-point value for the main process variable (in this case, steam pressure) set slightly higher than that of the other so that its valve will normally be completely closed (no flow). If the other (controlling) computer fails, its valve position will be frozen and, if the pressure rises, the other computer will take over. In practice, the operator will switch to manual and adjust the frozen valve to bring the new controlling valve to a more optimum position.

On the basis of their pioneering work with computers in connection with the NRU experiment in 1963 and their experience from Douglas Point, the Canadians believe that they can demonstrate that self-checking techniques can be relied upon to announce virtually any computer malfunction. Pearson remarks that "these diagnostic procedures have reached a high level of sophistication in our recent control system designs ---". From the available literature (13), these procedures and techniques are known to include the following:

- protection against bad drum-to-core transfers.
- core memory parity check. All detected errors lead automatically to a reload of the system from drum.
- execution time of all computer control and alarm functions are checked. If excessive, the function is recalled and tried again. If still excessive, the function is dropped and its outputs set to a safe value.
- all active functions are checked for actual execution.
- a periodic circulating data check which first outputs a reference value from a table in memory. This signal is passed through a D/A converter the output of which forms one of the regular signals to the analog input system. The resulting conversion back to digital form is compared with the original value. The test signal can be made to vary over the expected range of input. On Douglas Point, the analog value is fed to a strip chart for monitoring purposes. The program can be designed to check the executive program, the hardware timers, the interrupt system, memory, the instruction repertoire and the analog output and input systems.
- a hardware "watchdog" timer.

In addition, Smith and Morris (14) mention that all input data are checked for rationality and that other checks are made which protect against the execution of commands in a sequence other than the intended one.

They discuss also the background for the choice of a double computer configuration. As they state, redundancy does not help in the case of design faults, but, aside from this, they were interested in the practical overall reliability which could be achieved with a digital computer control system in a real industrial environment. In the case of Pickering which is a 4 x 500 MW station, they considered the idea of one computer per block with extra capacity in each to permit the taking over of two blocks in the event of a failure but concluded that this would not lead to a real economic advantage since most of the cost is in the process interface equipment. Instead, they chose to use a redundant configuration in each block. Both computers perform the critical functions while dividing the other tasks between them. The method of backup on duplicated tasks was also studied

with the result that both "parallel" and "standby" modes are used as was mentioned previously. In the parallel mode, the controlling devices, the feedback transducers and the computers are duplicated and control is shared continuously.

In the standby mode, both computers attempt to execute the control function simultaneously (in order to eliminate the updating of the backup computer at takeover time) but only the "normal" computer exercises control. To reduce differences in transducers, both computers have access to all input data and average them before use. A/D differences can be reduced by periodic re-calibration using the check loop discussed previously.

Pearson in 1972 (15) stated that the Gentilly system was on the way to becoming a fully operational unit with the double computer system functioning as planned. Computer switchover rate was down to once/week. The flexibility of the computer approach has made it possible to implement changes in control algorithms and interlock procedures as more experience was gained. In addition, transient and frequency response testing of the reactor has been possible with the computer both applying the disturbances and recording the results. A third computer (without process interfaces) has been acquired for training and programming. In addition, an on-line process simulator has been extremely valuable for initial program and hardware troubleshooting.

References - Section I

(1) Elektroteknikeren 1972:68:18 s. 409 "Datamaskiner for drift og kontrol af elsystemer".

(2) Electrical World 15/9-72 s. 102 "Computer Relay Shows Technical Worth".

(3) Electrical World 1/11-71 s. 48.

(4) Procesdatamaskiner på vest-tyske kraftværker. Procesdatamaskinegruppen, DEFU 1/12-72 - også en lignende beskrivelse af engelske værker fra 19/5-72.

(5) See HALDEN PROJECT semi-annual reports.

(6) Proc. IEE, IEE Reviews vol. 119, Aug. 1972 s. 1052.

(7) IEE Colloquium Digest 1971 "Some Considerations of Computer System Availability in Nuclear Power Plants".

(8) "Computer Systems in CEGB Nuclear Power Stations". R.R. Welch - Nuclear Engineering International 1/73.

(9) "Hartlepool & Heysham On-Line Data Processing Systems" - D. Hilton - Nuclear Engineering International 1/73.

(10) AECL 3452 "Computer Control in Canadian Nuclear Reactors" 1969. A. Pearson.

(11) "Nuclear Power Plant Control and Instrumentation". Proceedings of Working Group Meeting - 15-19/3 1971. IAEA.

(12) Information Processing 1968. "Dual Digital Computer Control System for Gentilly". Whittell and Bosomworth.

(13) "Heavy Water Reactor Symposium". IAEA 1968, article by Siddell and Smith.

(14) NUCLEX 1969 "Prospects for Computer Control in Nuclear Power Plants". J. Smith and D. Morris.

(15) Remarks at "IAEA Second Working Group Meeting on Nuclear Power Plant Control and Instrumentation". Brussels 5-8/4-72.

(16) "Computer Control at Pickering". T.B. Mahood - Nuclear Engineering International 1/73.

(17) "Minicomputers to Control Nuclear Generating Station" Canadian Electronics Engineering 9/72.

SECTION II

Important Trends and Technical Developments in Control Computing (1)

Several current areas of development in computing and instrument technology will have an impact on control computing over the next five years. It is doubtful whether such developments will be uniformly applied. A more likely course of events is that some of the developments will be applied to some systems.

Computer Price and Performance (2)(3)

The most significant development in computer technology over the next five years will be the gradual increase in use of large scale integrated circuits. The effects on performance can be large since more computing power can become available at the same price. A general improvement in reliability should also result from the reduction in power levels and number of interconnections. Reduction in prices will be less easy to obtain. Already for the larger computers, selling, support, and service accounts for a large part of the manufacturers expenditure. For a particular installation, this is not reduced significantly by using more advanced hardware. Hence price reduction for computers will be most noticeable in the minicomputer area, where there is less 'free' support for installation, software, servicing, etc., and where costs for such support can be spread over a larger number of sales.

Concentrating on the cheapest of the computers which can reasonably be programmed for general purpose use, this indicates a minicomputer with just 4 K words of store and a teletype. The basic cost of such equipment has fallen from about $ 15,000 in 1967 to about $ 3,000 in 1972. Over the same period, the price of 4 K 16 bit words of storage has fallen from about $ 8,000 in 1967 to about $ 2,000 in 1972. (The change is even greater if money values are reduced to 1967 levels).

In principle, the cost of a minicomputer processor could fall to very low levels comparable with the cost of say 10-20 LSI chips, $ 1-200. Such a development would rely on a very large market, and a significant reduction in support and service costs. This sort of pattern can be seen in the development of LSI processors for desk calculators, costing in 1972 about $ 50 for 3-4

chips. Such a development would not result in the sort of processor which supports many peripherals, and has a reasonable degree of software support for control. A more likely development relevant to the control market, is that more advanced and powerful computers will become available at about $ 4,000-6,000. Such computers will have more powerful instruction sets, better addressing structures, and better interfacing and interrupt equipment, without a significant increase in price.

At the same time as minicomputers develop, the speeds of memory will increase (to around 100 ns, at which point signal transmission speed begin to become significant) and the cost of memory will fall significantly. An order of magnitude reduction in cost to about $ 100 for 4 K words of store, is much easier to anticipate, since such stores could be used on a very wide range of computers, and thus reach a large market. At the same time, the normal store package for a minicomputer will increase in size. It will be more normal to fit 16 K or 32 K words of store to a minicomputer. Similar increases in the 'normal' amount of fast store will also be seen on the larger computers.

The significance of these developments for control computing are fourfold:

(1) It will be less necessary to 'optimize' program speed and size, by using assembly language for programming.

(2) Many applications which might at present be uneconomic, because of program size, will be limited instead by development and programming costs.

(3) If for security reasons, or to simplify development, it is desirable to split programs among two or more computers, then neither technological limitations nor hardware costs are likely to prevent such a split.

About four years ago, the first logical controller (4) appeared for use as a replacement for relay systems in repetitive/sequential control applications. These offered a flexibility advantage in that their programs could be altered to suit the actual situation. In addition, it was relatively easy to interface them to higher-level computers for monitoring and diagnosis. They cost between $ 5,000-12,000 and incorporated a central processor

employing combinations of discreet and integrated components which executed a program stored in a read-only memory to perform the required counting, sequencing, timing and logic functions. They also included interfaces designed to handle directly such items as contactors, solenoids, etc. and, in general, were capable of operating in an industrial environment. Execution speeds were relatively low compared to general-purpose minicomputers but, in the following years, many different models of these industrial controllers appeared on the market.

An important and related development within the past year or so has been the emergence of low cost "micro" computers (5), manufactured with MOS/LSI techniques which can offer significant savings insofar as central processor costs are concerned. Among other things, these offer instruction sets which are more extensive than the models mentioned earlier and again are potentially useful in dedicated applications. In power plants they could be used, for example, in the more standardized tasks such as motor, pump and burner control where the ultimate in speed is not required.

A typical micro-processor* today consists of three 40 pin chips and costs about $ 300. Others are already priced as low as $ 50 in quantity. However memory and peripheral costs are far from insignificant and, in addition, programming is more awkward than on the larger machines. Since semiconductor firms rather than computer manufacturers are producing these units, proper support facilities are not as extensive. However, these units are a potentially inexpensive and flexible tool for implementing all sorts of dedicated control system functions. See (19) for one of the first applications - "A digital brain for a digital valve".

*Another recent related development is the appearance of the C-MOS (complementary metal oxide semiconductor) circuit as a competitor (or supplement) to the other commonly employed types of logic. C-MOS offers the advantage of low power consumption, high conducted noise immunity and operation from a single power supply. Predictions are that this technique will win wide acceptance in the future in applications where ultra-high speed is not required.

Backing Store

Disc (drum) memory is unlikely to decrease very much in cost per unit although recording densities will rise. This will not have a significant effect on control computing. Of greater importance from the standpoint of reliability are the current programs in the US and Japan which aim at the development of non-mechanical substitutes for disc and drums at comparable (and even ultimately lower) prices (6). These replace the mechanical motion of a moving media with the intrinsically faster movement of magnetic domains in a stationary media and use shift register techniques to access the contents. The most promising approach (so-called magnetic "bubble" memory) permits a high packing density (approx. 1.5×10^5 bits/cm^2 have been achieved) and comparable shift rates (3 megabits/sec have been reached). Access time is proportional to shift register length. In addition, these units can be made so that their contents are insensitive to power failures.

Actually the first commercial version of magnetic domain memory appeared 3-4 years ago. Its bit price is about 0.25 cents - the ultimate goal is 0.001-3 cents, or about 1/10th the cost of a disc.

One should also mention the current availability of so-called "silicon disc" memories (7) which are rather expensive (1-2 cents/bit) equivalents using MOS shift registers connected so as to simulate the mechanical rotation of a disc or drum. An advantage is their high word transfer rate and low access time. Another advantage which they share with the magnetic domain approach is that alternate structures are possible which can optimize performance for a specific application. At any rate, it is quite possible that the intensive work being done to reduce random-access semiconductor memory costs will also affect the "silicon disc" approach and make it attractive in special situations.

For the sake of completeness, mention should be made of the intensive development work being carried out on electrooptical techniques. However the current consensus of opinion is that their entry into the market lies beyond the time scale of this report. In addition, their preferred areas of application are still somewhat unclear at this moment.

To sum up, the impact of such developments in mass memories for control computing is that random access backing store in the most useful size, should become cheaper and more reliable. It will still be necessary to make special provision for storage failure, either by duplication of stored data and programs, or by providing rapid reinitialization procedures. But the cost of backing store duplication should be lower, and the effectiveness increased.

The increased speed of such memories will be significant in improving performance for systems which move programs between backing store and main store, or which store large tables of variables. The closer match between main store and backing store speeds will make the use of paging organization more attractive, leading to considerable simplification in the design of systems using large data tables, or large programs.

Communication and Bus Systems

One of the most significant changes in minicomputer architecture over the past three years, has been a change to bus structures for accessing both main storage and peripheral interface registers (8)-(11).

The effect of these changes has been to enhance system flexibility and expandability and to make equipment interfacing, and especially, direct memory access, both easier and cheaper. However increases in store and processor speeds have made the signalling time along a bus more significant. Therefore we can expect to see an increase in the number of busses per central processor, and the number of ports per memory module. This will allow easier overlap in fetching instructions, and reduce the direct memory access interference with program execution (important for discs, and if processor store is used for refreshing displays). It will also enable multiprocessor architectures to be implemented more easily.

Bus systems have also been developed for interfacing instruments and peripherals, independent of the memory or peripheral access channels.

The Camac system (12) is a parallel data bus system, which has been standardized. Implementations of the bus controller have been developed for several computers. The Camac bus serves

as a multiplexer for a potentially large number of instruments. The instrument interfaces need only be developed once, new interfaces are not needed for each new computer type. When a new computer is developed, all that is necessary is to develop a new bus controller.

The main advantage of such a system is that interfaces can be standardized, and this has resulted in a wide range of choice of instruments for nuclear measurements, on many computer systems. This particular system has a higher data capacity than is required for many process instrumentation applications (24 bit lines with a register reading rate between 1 and 100 µsec). Also the flexibility in choice of computer or of instruments is not so likely to commend itself to manufacturers used to supplying ing complete control systems of their own design. However, it could prove very useful to a potential user with several process control applications.

An alternative form of instrument interconnection has become commercially available, for use either with or without a computer (13). Its objective is to reduce the costs of cabling, and to reduce the noise sensitivity of instrument connections. The principle is to use just one high frequency cable configuration for transmission over long distances, and to use multiplexers to provide individual lines to instruments, etc. relatively close to their actual location.

Many alternative configurations are available over a wide range of data transmission capacity. The highest capacity systems use coaxial cable for serial synchronous signalling, at about 2 m-band to reach the multiplexers. The multiplexer connects to analogue to digital and digital to analogue converters, or to digital input and output stations, via twisted pair lines.

The highest capacity systems can sample 5,000 analogue inputs or about 60,000 discrete inputs, per second.

A novel system designed by Hitachi (14),(15) provides pair of coaxial cables, in a loop up to 1 km long. Up to 100 multiplexers can be situated on the loop, with a maximum of 5 analogue and five discrete inputs or outputs per multiplexer. By using several such small multiplexers, the distance between instruments and the main data channel is further reduced. Communication is invulnerable to a single break in the data channel.

Coupling from each multiplexer station to the data highway

is accomplished via special transformers which provides isolation, common-mode rejection and fail-safe operation in the event of a station failure.

For power plant use, the reliability of a single cable communication system would need to be carefully considered. However, it should be possible to increase communication reliability above present levels by duplicating communication lines (and possibly multiplexing equipment) without leading to excessive cost.

A very important feature of these systems is that they can be designed to stand alone and operate without the computer.

The impact of developments in communication of data on control computing will be very significant. One of the major factors which affects reliability for computer control systems at the moment, is unreliability and noise sensitivity in the interfacing equipment and in interconnections. By reducing crowding, and reducing the length of analogue signal transmission, these problems should be reduced. Additionally, where such communication systems are introduced in order to save cabling costs irrespective of computer control requirements, one of the major obstacles to use of computers will be removed.

Process I/O

This portion of a computer control system is one of the most expensive and most difficult to design. The large number and types of channels involved and their various locations within the plant proper require careful attention to cabling, shielding, back-up, etc. to maximize data security and reliability.

Conventional techniques today employ some form for multiplexing of analogue and digital signals. The cost/channel for the former using reed relays, filters, and "flying capacitor" isolation to solve noise and common-mode problems are high. Newer systems which employ FET switches with zener-diode and fuse protection usually employ several levels of multiplexing to reduce the effects of capacitance and leakage and thus obtain high scanning spreads. They are also expensive.

More widespread use of electro-optical devices is likely in this area, basically as isolating units to remove common-mode and grounding problems and improve plant security in the case of

physical accidents. Ultimately, it may become feasible to use linear light-diode coupling for analog transmission.

However, changes in the cost of digital electronics are likely to affect the way that instrument and actuator interfacing is carried out.

Firstly, analogue to digital converters, amplifiers, and shift registers are becoming much cheaper. If digital conversion equipment were included in each analogue instrument, the cost could be as little as $ 100 per instrument, comparing favourably with present day multiplexed analogue to digital converters. The advantage would be simpler wiring, and by using redundant data transmission codes, less noise sensitivity.

Finally, it is now economical to implement two and three-term controllers using digital electronics. The advantages lie in their simpler coupling to computing equipment. Actually, if these units were part of a digital communication system with corresponding digital instrument transmitters, it would be possible to produce a digital control system capable of working without a computer.

Seen from another angle, if one extends the idea of distributed processing using the "micro" computers mentioned earlier, the concept of centralized control begins to disappear and the distinctions between interfaces and computers become also less clear. For example, process data are then available for remote manipulating at their points of origin via arrays of communicating dedicated machines using standard programs. This results also in lower traffic demands for information and coordination.

ICI's MEDIA system (16) illustrates the start towards such an approach. This is now being produced commercially.

Although all of these developments are possible, it is unlikely that they will be introduced simultaneously in any applications. The coordination of development would be difficult, and the risks involved in making many developments at one time are large.

Display/Controls Interface

The trend toward centralized and integrated control room configuration will continue with the computer playing a vital

role in the management of the display/controls interface. Many major process instrumentation firms such as Siemens, Brown-Boveri, Foxboro and General Electric (see, for example, their NUCLENET 1000 system) are active in this field. Developments in raising the level of automation employed in future plants will have a strong and direct influence on the functions, layout and communication facilities which will be incorporated.

The CRT will continue as the major device for display although expectations are that the plasma display may emerge as a serious competitor in view of its potential for large-screen colour presentations without the need for external refreshing if the price can be made comparable to that of an equivalent TV tube-based system. Units have already been built as large as 40 x 40 cm with a total of 512 x 512 three-colour display elements (17).

Light emitting diodes (LED's) (18) can also become useful for displaying small amounts of alpha-numeric information - or ultimately as status displays - now that colour limitations are disappearing. Liquid-crystal displays, the other major contender at the moment, do not seem likely to have a major impact in the control room.

Present use of light pens, tracker balls, etc. for direct operator interaction with the information displayed on the screen will give way to systems which permit simple finger pointing without the need for special devices. However, wide-spread use of direct voice command recognition is less likely.

A special problem which is named quite frequently in discussions on "paper-less" control rooms is that of obtaining "hard-copies" of relevent process data when desired. These could then form part of the archive on station performance which could become a valuable aid during many phases of subsequent plant operation.

The solution to the "hard-copy" problem has not really been solved economically as yet although several devices are now available on the market with prices from about $ 5000 and up. There are many relevant factors to consider such as initial and running costs, time required to make a copy, copy size and permanence, need for a special CRT, etc. The least expensive solution today is probably still the polaroid camera - while a technical break-through is said to be necessary before a reasonable cost/performance ratio can be achieved.

In summary, the overall implication of the developments mentioned earlier is that costs should not raise substantial obstacles in the way of providing sufficiently flexible and redundant control room facilities.

References - Section II

(1) Electronics 13/9-71. Survey article s. 61.

(2) LSI - Implications for Future Design and Architecture - S.F. Dennis and M.G. Smith. SJCC 1972.

(3) "Approaching the Minicomputer on a Silicon Chip - Progress and Expectations for LSI Circuits". H.G. Rudenberg. SJCC 1972.

(4) "Programmable Logic Controllers". G. Lapidus. Control Engineering April 1971 and N. Andreiev. Control Engineering Sept. 1972.

(5) "MOS/LSI launches the Low-Cost Processor". G. Lapidus. IEEE Spectrum Nov. 1972.

(6) "Review of Current Proposed Technologies for Mass Storage Systems" R.E. Matick. Proc. IEEE vol. 60 no. 3, 1972.

(7) "Silicon Disk Memories ..." S.W. Fields. Electronics 24/5 1971.

(8) "Common Bus Structure for Minicomputers Improves I-O Flexibility". P. Janson. Control Engineering, Jan. 1971.

(9) "Evolution Breeds a Minicomputer ...". R.J. Clayton et al. Electronics 11/10/71.

(10) "Direct Function Processor". S.B. Dinman. Computer Design. March 1970.

(11) "Stored Program Control of Exchanges Using a Multiprocessor System". J.M. Cotton. IEE Conf. Pub.

(12) CAMAC Specifications. "A Module Instrumentation System for Data Handling". EUR 4100e. "Organization of Multi-crate Systems". EUR 4600e. "Specification of Amplitude Analogue Signals". EUR 5100e.

(14) "Line Sharing Systems...". R.L. Aronson. Control Engineering. Jan. 1971.

(14) "A Data Highway System". F. Inose et al. Instrumentation Technology. 1971:18:1.

(15) "What's New in Automatic Process Control". H. Simon. Chemical Engineering. 11/9-72.

(16) "MEDIA - A Continuous Digital Process Control System". J.R. Halsell et al. IEE Conf. Pub. 85, 4/72.

(17) "Electronics Review". Electronics 9/10-72, s. 39.

(18) See for example EDN 1/7/72, s. 24 or "Special Issue on Information Display Devices". IEEE Transactions Vol. ED-18 No. 9, 1971.

(19) "Digital Brain on a Digital Valve". A.W. Langell Jr. Control Engineering. Dec. 1972.

SECTION III

Developments in Software and Programming

The technological developments which have been described previously will have a direct impact on the software which will be required as well as on the tools and methods which will become available for generating this software. However, to indicate present practice and experience, the results of a recent American survey (1) of process control users may be of interest. They indicated that only about 28% utilized a higher-level language (mostly FORTRAN) while 25% still employed direct machine language and the rest assembly language for their applications programming. This can be contrasted with Danish experience which rests on the use of ALGOL or a macro-assembler approach for those systems which currently are operational. The disadvantages of lower-level languages are well known. The predicted developments in the price of computer store should remove any lingering reservations about the need to save on memory space by using machine or assembly language.

However, the universally acceptable and implemented higher-level equivalent is not yet available and there are few signs of its imminent appearance. Typical of the efforts underway in this direction are those of the Purdue Workshop on the standardization of industrial computer languages which has been active for the past four or five years in the following areas:

- extension of FORTRAN (because of its popularity) to serve as at least one of a set of available procedural languages for process control. This standardization effort is expected to be complete in 1974-5 and represents the short-term solution to an application programming language
- development of a so-called long-term procedural language expressly for real-time applications (see Pike (2)). This is an international effort and a single unanimous result cannot be expected to emerge within the time era relevant here, although implementations of various specific proposals are likely - indeed, they have already occurred (3).
- development of problem-oriented packages which perhaps,

through use of macro-processor or other techniques, will permit each user to define his own application-based language. Here again, the expected reduction in hardware costs will make this approach more attractive.

For at least the next five years, however, process computer systems will continue to be manufacturer-dependent. Nevertheless, hardware developments and the influence of, for example, micro-programming on the ability of computers to execute in hardware in a flexible and alterable (if desired) way that which today must be accomplished via software will supplement the trend toward manufacturer-supported high-level "standard" programming languages and program packages for their main market areas.

An increased use of distributed computers of various sizes and complexity in process control applications creates a somewhat altered environment for programming and will probably lead to more widespread use for the "software factory" idea (4) & (5). This consists of a computer for the high-level language, a utility library of building block software modules, powerful debugging facilities and a host computer capable of supporting all of these. The output of the "factory" is an object program capable of running on the specific process computer with also the possibility for loading a writable ROM in the target machine with the optimum instruction set. The possibility for building up and continually expanding the library of software modules in the host is particularly attractive - this could include

- components for the development of special language processors
- operating system modules
- on-line application modules
- user interface modules
- etc-

As an indication that this is far from a remote possibility, for example, the latest IFV system will be programmed on a large host computer while the resultant object programs will be executed on the actual smaller process machines.

Program Testing and Check-out

Although techniques for modular program development are still not widely used to full advantage, we should see their use increasing rapidly over the next five years, along with the move away from assembly language programming.

Two sorts of technique are possible for dividing software into modules - division into subroutines and procedures, and division into 'tasks' or 'processes'. The second of these will become more popular than today, as multiprocessor computers become more common for control computing. We can expect to see much more powerful program testing facilities, allowing a high level language approach to debugging. The presence of displays during program development will encourage the use of more check data during testing. The effect of this should be to make program development more rapid, and less error prone.

One of the major areas of development in software techniques over the past two years has been in program proving techniques. These allow a programmer to check the consistency of a program with its specification. The techniques still require excessive effort and cannot be applied to complete systems. But within five years, knowledge of such techniques should have spread far enough to have been used in checking the more complex parts of some systems. At the same time, the use of such techniques should lead to improvements in quality of program specification and design.

The overall effect should be both to decrease the time for debugging of a system, and to increase the size of software systems without making them unmanageable.

References - Section III

(1) "A Survey on On-Line Control Computer Systems". E.J.Kompass. Control Engineering. Jan. 1972.

(2) "Procedural Language Development at the Purdue Workshop on the Standardization of Industrial Computer Languages". H.E. Pike. IFAC 5th World Congress 1972.

(3) IFAC Report. H.A. Spang III. Automatica, Vol. 8, pp. 493-8. 1972.

(8) "Future Trends in Software Development for Real-Time Industrial Automation". H.E. Pike. SJCC 1972.

(9) "Future of Minicomputer Programming". D.J. Waks et al. SJCC 1972.

SECTION IV

Control Computer Structures for Power Plant

Computing power for power plant control can be provided in a great many ways, with different degrees of distribution, and different levels of redundancy to ensure reliability.

Computing equipment might in some cases be able to offer relatively intangible benefits (for which the value is difficult to determine, although it may be large). Examples are increases in control system flexibility (important during commissioning and for plant modifications); improvement in control quality (though this may be difficult to achieve); better presentation of information to the operator; and reduction in the number of operators required.

However, the objective here is to find the costs of a computer control system, since this may now be lower than the costs for conventional equipment. There are some difficulties in using computing equipment for control purposes. One is the cost of software. Purchased software is not generally suitable for power plant control, except in the case where a completely packaged control system is purchased from a manufacturer with experience in computer control of power plant. Some manufacturer supplied operating system, compiling, and utility programs, are useful. But for a fully computerized system, about 100 K of additional programs are required, i.e. about 10-20 man years effort, or between $ 80 and $ 360,000. A good proportion of this sum would be required for design of an equivalent analogue control system, but if analogue backup equipment is provided, the software represents a pure excess cost.

The cost of software, and the cost of gaining experience, can be greatly reduced if one team is used to produce several systems. If similar machines are used, or software is written in a standard high level language, costs and software error rates may be further reduced, by reusing software.

A further problem with computer control of power plant is the rapid rate of change of computer technology. This makes redesign of systems desirable over periods as short as four years, and limits the extent to which software can be reused for new plants.

A final problem with computer control is that of software errors. They are generally not critical, in that they can be quickly cured by restarting a computer system. But they represent an operational inconvenience, and may occasionally lead to tripping the power plant. Special care needs to be taken in design to overcome these problems, and additional software and hardware is required.

Reliability Requirement

Most of the individual units such as processors, store modules, and multiplexers in control computer systems have a mean time between failures of between 10,000 and 30,000 hours. Repair times depend on working conditions, but vary between 1 and 24 hours, usually. Exceptions to these general rules are line printers, typewriters, disc stores, and very large processors.

A convenient way to determine the required level of redundancy in a computer configuration, is to evaluate the capitalized cost of failures for the component. If this is greater than the cost of the component, an additional redundant unit should be added. If components are already duplicated, an alternative way of increasing reliability is to allow cross coupling, so that, for example, if one disc store and one processor fail, a second store and processor can be interconnected easily, even if they were not usually used together. An objective of computer system design should be that if a component fails, and a replacement is available, replacement should take place sufficiently quickly that it is unnecessary to trip the power plant.

The costs due to plant shut down can be arrived at in the following ways:

- It is more expensive to produce electricity in older, or reserve plant, or to buy from other supply authorities.
- More capital equipment is required to provide reserve capacity.
- Costs for spinning reserve and warm standby operation of some plants.
- A cost in the residual danger of a major system breakdown, resulting from several plant failures close in time.

Some of these costs are difficult to determine, but the largest items are for spinning reserve and standby capacity. The optimum level of spare capacity depends largely on plant availability.

Costs of critical failures can be estimated, using for example, the approach given in (1). These costs can serve as a guide for determining both whether control system redundancy should be used, and what form it should take. Ref. (1) gives $ 25-50 per megawatt day as an approximation to the financial loss due to plant shutdown. These costs are somewhat lower than the German values, given in (1) and approximately the same as the CEGB's (Jervis).

They can be expressed in terms of unavailability (MTTR/(MTTR+MTBF)) in that 1% of unavailability (approximately 100 hours or 4 days per year) is equivalent to ($ 25-50) x 500 mW x 4 days = $ 50,000-100,000 per percent of unavailability per year. Thus, using (1)'s terminology, an improvement of 1% in availability is equivalent to a capitalized saving of $ 320-640,000. A value of $ 500,000 will be assumed in the examples given later.

As an example of how this works out in practice, a minicomputer processor has a mean time between failures of about 10,000 hrs. and a mean time to repair of about 10 hrs. If it is essential to plant operation, it contributes about 0.1% to plant unavailability, or about $ 50,000 in capitalized costs. Duplication up to this cost is worthwhile, unless there is some simpler and cheaper strategy for keeping the plant operating. In practice, such duplication would cost about $ 10,000, but provision of a limited (analogue) backup system for the more rapidly varying plant variables, and manual control facilities for the other variables might be even cheaper.

Control Hardware

The number of possible arrangements of computing equipment is very large. An attempt has been made in the following pages, to make a fairly thorough comparison of the different structures. Some points of technical interest concerning the most promising structures are also made.

The base line for the control system design is a 500 MW con-

ventional power plant. Conventional, fully automated instrumentation of such a system involves

800	discrete output signals
1000	analogue measurements
1300	discrete signals
30	analogue output signals
50	PID ratio controllers
30	A/M stations
40	summing amplifiers
30	high/low selectors and limiters
7	sequential controllers - Turbine run up
	Start up
	Shutdown
	Load changing
	Feed pump control
	Burner control
	Synchronization

The approximate present day costs for computer hardware components are as follows:

Miniprocessor, 16 bit with clock	$ 6,000
4 K words of store	$ 2,000
Peripheral multiplexer, 16 channel	$ 5,000
2 M byte disc unit + controller	$ 10,000
Line printer	$ 18,000
Console typewriter	$ 3,000
Raster display, with own store and driver	$ 12,000
Disc store duplexer	$ 2,000
I/O bus switch	$ 2,000
8 way store multiport unit	$ 5,000
Paper tape equipment (for programming) reader/punch	$ 4,000
Cassette tape equipment (for programming)	$ 4,000
A/D converter, 1000 channel	$ 80,000
D/A converter, 32 channel	$ 10,000
Digital input/output, 2000 channel	$ 70,000

Mean times to failure and repair times can be estimated as follows:

	MTBF, hrs.	MTTR, hrs.
Miniprocessor	10,000	2
4 K block of store	10,000	2
Peripheral multiplexer	20,000*	4*
Line printer	1,000	4
Console typewriter	1,000	2
Disc store	1,000	10
A/D converter, 1000 lines	200-1,000	1
*8 way store multiport unit	10,000	2

*estimated by comparison with processor.

The figures are based on a range of predicted and observed values for modern equipment, the values being 'typical'. For design of specific systems, manufacturers' data should be used. The MTTR values assume that maintenance staff are always available, with a full set of testing aids, including test software. For most systems, there are a few 'unexpected' failures with extremely long repair time, involving delays of days, or even weeks.

Computer Configurations

To make evaluation of different computer configurations simpler, the overall computer system has been divided into the following subsystems:

Control console
Computer
I/O systems.

For each of these areas there are several possible alternative design solutions. The result is a very large number of system structures. The approach taken here is to select the best alternatives for each subsystem, and combine them. In some cases, there is no freedom to combine good subsystem alternatives in this way, since some alternatives in different subsystems are naturally paired.

The tasks assumed for the control system include:

- Direct digital control of plant variables
- Sequence control, and display of progress
- Display console support
- Alarm monitoring and display
- Reporting/supervision
- Logging
- Sequence of events analysis after incidents

Control Console

It is assumed here that raster displays, with 16 K bytes of semiconductor storage for each display are used, since these represent the best solution to the display problem currently. Commercial colour television monitors are used as final elements in the display system. Multicolour plasma or multiphosphor CRT displays may be available by 1974, with sufficient reliability. They should enable costs to be reduced, and the discrimination and hence density of information, on the screens, to be improved.

It is assumed for the purpose of the examples here that five displays are required. Displays of this kind have a mean time between failure of about 2000 hours. Assuming a repair time of four hours, the availability is 0.2%, with a capitalized of $ 100,000. At least one spare is justified. The availability of a group of six units, five of which are required for convenient operation is 0.004%, with a capitalized cost of $ 2,000. Provision of further redundancy is not justified, in terms of complete units.

In practice, a large proportion of the display system failures are likely to be within the display monitors themselves. Spares, and extra units for closed circuit television, monitors, cost about $ 400. They could be made interchangeable using coaxial plugging. Both displays and console keyboards should be arranged so as to be easily movable, in order not to disturb the control configuration while some equipment is being required. It is possible to envisage operating the system with reduced control capabilities, if more than one of the display systems should fail. Software switching is used to move pictures between displays.

The essential components of a raster display system are shown in Fig. 3. A configuration is shown in Fig. 4 with two display processors provided. The processors serve to translate display

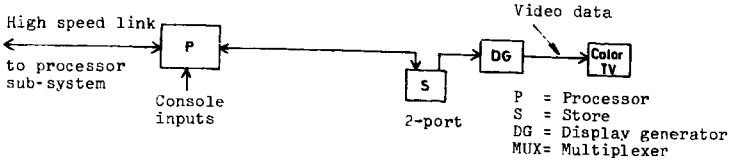


Fig. 3. Essential Components for raster display

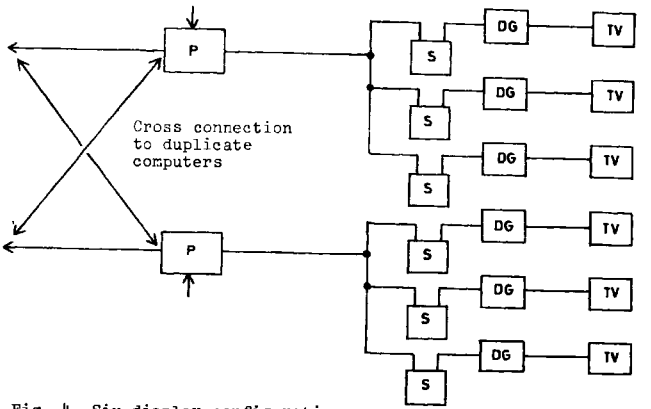


Fig. 4. Six display configurations

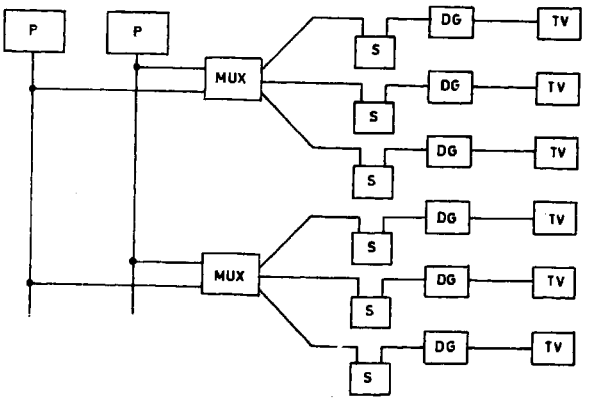


Fig. 5. Multiprocessor connection to displays

data from the compressed form used in other parts of the system into point or vector form used by the displays. The unavailability of the processors individually is approximately .02%, and of the pair (one processor and one display failed) is 4×10^{-5} %, with a capitalized value of $ 200. Further redundancy is not justified, provided it is possible to operate in a limited way with only three displays, while repair takes place. Given the assumptions made sofar, the best way of adding redundancy to the system is to provide an extra display on each of the processors, if operation with only three displays is considered difficult.

A fairly high speed data link to other parts of the control system is required, if pictures on the displays are to be changed at a sufficiently high speed.

The cost of a system like that of Fig. 4 is $ 90 K, based on the costs for one commercially available system. A marginal saving can be made if a multiprocessor system is used, by combining the display processors into the rest of the multiprocessor system (Fig. 5).

Of particular value to a user would be a method for generating new display programs easily. The amount of software involved for accepting pictures from a main computer, for providing a good display interface, for using tracker ball or similar pointer devices, and for picture switching, and for providing a general keyboard handling program, is about 4 K. In addition, about 4-8 K of display store is required to hold pictures. The software required for new display hardware might take 2 man years, to provide the basic display facilities. In addition, each picture to be displayed required 1-2 man months of design, programming, and editing time, even when the basic principles of design are well understood, and aids to picture generation have been provided.

Fig. 6 shows a possible data flow scheme in display software. Significant decisions to be made in the design of the display software are the degree of structuring in the picture file and in the picture formats; whether the data transfers should be active (fetch) or passive (send), which affects the failure properties of the software; and how to organize error recovery in the case of hardware or software failure. Note the picture location table, required to enable pictures to be moved from one screen to another in the case of failure. This should also allow one picture to be

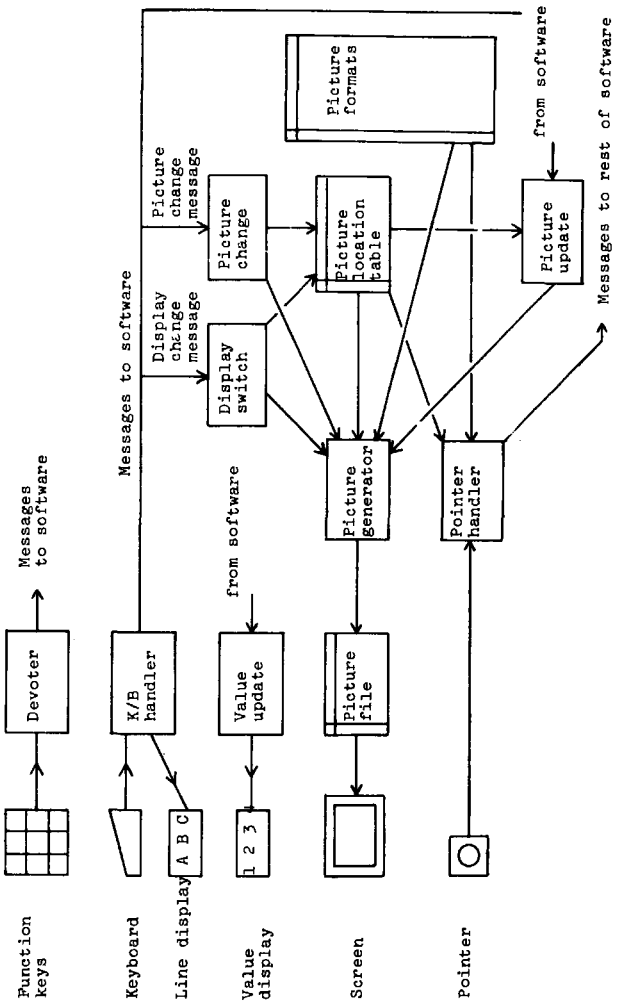


Fig. 6. Data flow in a picture display software.

replicated on several screens.

As was stated earlier, computer-controlled control rooms are now commercially available. The important issue is the effect future developments in the degree of automation employed in process plant will have on control room function and requirements.

Processor Subsystem

An assumption will be made in describing different processor structures that direct digital control is used, at least as far as the primary (non-standby) control is concerned. One way of justifying this assumption is that computer data logging and data display are already provided in many power plants, and the additional cost to provide capacity for direct digital control is very low. Savings may then result from reducing the amount of analogue control equipment. It may be possible to reduce the overall cost of control equipment by using a completely digital control system, especially if advantage can be taken of reductions in cabling costs by using remote signal multiplexing. If a completely digital system is provided, the extra costs incurred are mostly in providing redundant equipment. As will be seen later, the dependence of the computer control system on a single, complex, computer system results in inadequate reliability.

The basic hardware requirement for the processor subsystem is a single miniprocessor; disc store; a control typewriter; line printer for logging; cassette tape and paper tape equipment for programming.

Several suitable minicomputers are available, with prices ranging between $ 3,000 and $ 12,000. The cost of processors is a relatively small part of the overall control system costs, and the choice should be made on the availability performance and cost of the other equipment associated with the processor; the availability of good control software or a good operating system and programming language; features for protection and ease of programming which make programs more reliable; and ease of repairability of all of the components in the system. A price of $ 6,000 has been used as a basis for comparison here, because there at the moment are few systems commercially available with outstanding advantages, above this price.

The amount of processing power for direct digital control, supervision and data logging, does not represent a large load for a modern miniprocessor. The load has fairly stringent timing requirements however. Changing pictures, alarm analysis, and updating of trend curves, can produce a heavy, computational load during a short period. Careful attention must be paid to setting program priority levels. The problem is reduced in multiprocessor configurations, where the display generating computer is also available to take other peak loads.

The amount of store required for the computer depends very much on how much of the program and data is stored on disc. This is partly a question of reliability. Historically, most of the application programs for a system, and the process data, have been stored on disc in large process control systems. However, disc store is one of the least reliable components in a computer system, with relatively difficult repair and replacement problems. With control relying on the proper working of a disc, two disc stores are easily justified. The unavailability is then 0.01%, with a capitalized value of $ 5,000. A third unit is not justified on the basis of these costs, but it seems worthwhile to seek alternative ways of increasing reliability.

An alternate approach, which is especially attractive for the redundant system structures to be described later, offers a higher availability for "essential" functions and, at the same time, can relieve timing problems associated with access to backing store by providing sufficient main store to permit these functions to operate without backing store. The disadvantage in a single processor system is that backing store is still required for system re-load after a failure so that dependence on this critical element is still a factor. This dependence can be minimized by incorporating protection features to reduce the propagation of errors throughout main store and by using a structural approach to recovery procedures which uses backing store only as a last resort.

It is important with an expanded fast store to compress process data, sequential control programs, picture formats, trend data, etc., using table and list techniques. The success of the approach will depend on the success of these techniques, and experimental developments of new control aids may necessi-

tate extra store. The direct control, alarm reporting, logging, supervision, and display programs will be required to reside in main store (logging of important variables direct to line printer can be used).

Assuming that high level language programming with a moderate amount of error checking and recovery software is used, the store requirement for a process control system of the required capability, is approximately

8 K	words	operating system
10 K	words	process data
8 K	words	essential applications programs
4 K	words	background program execution area
4 K	words	picture formats
2 K	words	display generation programs
2 K	words	frequently used trend data
2 K	words	messages
2 K	words	sequential control tables
42 K	words	
48 K	words	with reserve.

Less flexible systems with half this quantity of store have been constructed, using disc storage to allow a degree of program swapping. Addition of a cheap ($ 1,000) 'floppy disc' store can give an extra capability for running less frequently used programs, during repair of the main disc, but will generally not be sufficiently fast for logging.

The unavailability of a single processor subsystem, consisting of a processor, 48 K store, disc, and keyboard is the sum of the individual unavailabilities.

	Price	UNAVAILABILITY	
Processor	$ 6,000	0.02%	
48 K store	$ 24,000	.24%	
Disc store	$ 10,000	1.0 %	
Control keyboard	$ 3,000	0.02%	
	$ 43,000	1.3%	full function
		0.3%	without disc

In practice, better levels of availability than this have

been achieved at some installations. However, in many cases there are transient failures and software failures, which require good recovery and restart facilities, if such high availability is to be achieved. The capitalized value of unavailability for a complete processor subsystem, even without a disc, is ∿ $ 150,000, and some redundancy is justified.

Analysis of event sequences (post incident analysis) is a special task, in that although reliability is not critical, special equipment is required. The equipment required consists of special multiplexers in order to buffer about 1000 incoming event signal lines, and a small computer to sample these lines. There is some advantage in connecting this subsystem to the computer system, to allow access to the display subsystem, and in some cases, to gain in reliability by allowing the event recording computer to be a standby for the control computers (shedding the event recording task).

Redundant Structures

There are two forms which a central, redundant computer system can take, the dual structure and the multiprocessor structure (other forms, with distributed processing, will be considered later).

The dual system (Fig. 7) consists of two similar processor subsystems, connected by a switch or watchdog timer. Whenever one computer is active, and capable of running the plant, it periodically updates a register in this switch, and so indicates to the other computer that it must remain in a standby role. Complete failure of the active computer, or a call of an error routine, or a manual signal from the operator, results in the switch not being updated, and the standby processor can take over the active processor functions.

The basic unavailability for the single processor system, without disc store, was shown to be 0.3%. The unavailability of the equivalent duplicate system is 0.0009% for "essential" functions with a capitalized cost of $ 450. Care must be taken in organizing the switching, multiplexing hardware in this configuration, and in perfecting the protection and recovery software, because there is a source of common mode failure in that programs and data are shared on a single disc. Loading a faulty copy

of a program can cause complete failure of the system. The low unavailability for essential programs involves an extra net cost due to the addition of 2 x 24 K of fast store and a disc multiplexer minus the cost of one disc (or in all about $ 20,000).

If a dual disc system is used, the problems of common mode failure are avoided, or, if both discs are connected to both processor subsystems, reduced to a negligible level. For a simple dual system with two discs, the unavailability is 0.012% with a capitalized value of $ 6,000. For a cross coupled system, with both discs connected to both processors (Fig. 8) the unavailability is 0.011% with a capitalized value of $ 5,500, so the advantage of being able to use both discs on both processors is at least marginal, from an economic point of view.

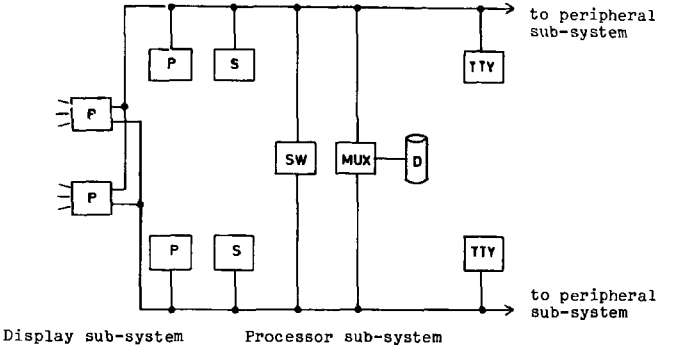


Fig. 7. Dual processor system.

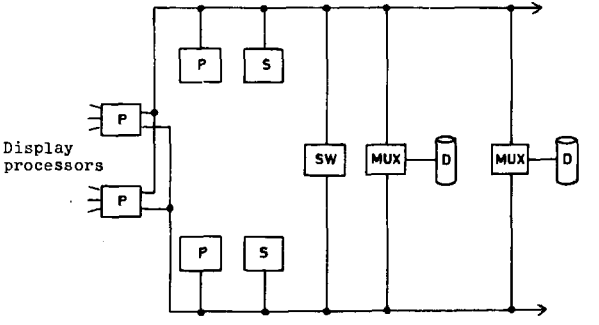


Fig. 8. System with dual processors, and dual, cross coupled,discs.

A dual system can be operated in either of two ways. The first requires only one computer to perform the control tasks, the second being available for background work. If the active or control computer fails, the standby or background computer can be loaded with programs, and started on the control tasks. In a modern system using disc store for programs, the time for this reload process can be reduced to a few minutes.

The second way of operating a duplicate computer system is for both computers to run at the same time, performing all the control calculations. However, output is provided by only one computer, depending on status of the watchdog time/switch. In this parallel operation mode, recovery from failure is much more rapid, because all process data is available instantly to the standby computer, without an initial period for loading programs and gathering initial values of process data. A disadvantage is that twice as much data transfer capacity is required in the process data input system. If such a system is operated with a single disc, very great care is required in software design, to avoid the possibility of common mode failure for the duplicate processors.

Dual computer systems are available from process controller and computer manufacturers. Software can be purchased for systems where one computer serves as a backup, or standard control software can be modified with little difficulty. For the parallel mode of operation, special applications software is generally required.

The cost of a duplicate system including two discs, two processors with 48 K of store in all, three console typewriters, paper tape, cassette tape, and two line printers, is approximately $ 107,000 (see Table 6) (the line printers, paper tape, and cassette tape are mounted in the input-output subsystem, but are included here for convenience - being part of the computer equipment, rather than the 'process interface'). A separate event recording computer costs approximately $ 30,000 without any special display facilities.

A multiprocessor system offers the potential for very high availability, without an excessive cost, because full interchangeability of modules is inherent in the structure. For example, if three store modules of 16 K words each are required in the basic system, and two spare modules are provided, then the unavailabil-

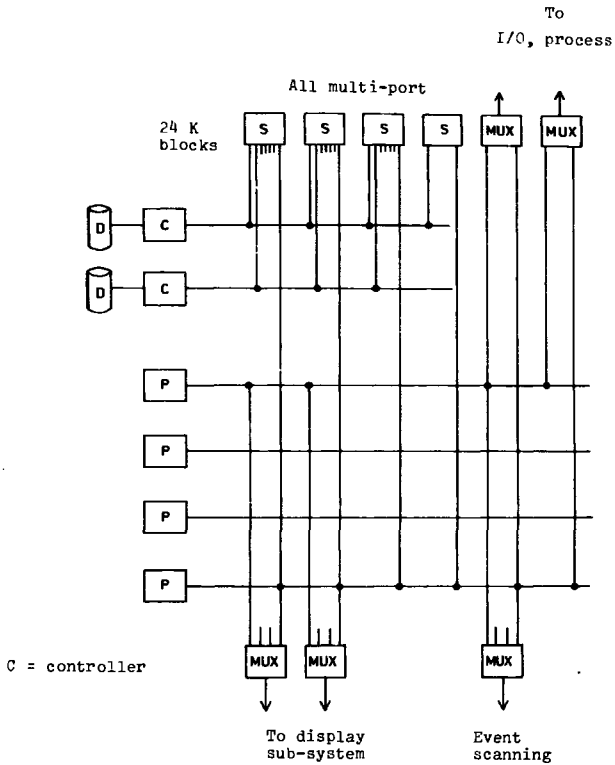


Fig. 9. Multiprocessor system with control and display functions integrated.

ity due to store module failure is approximately 3×10^{-9}, that is, three days in 100,000 yrs. However, the increases in availability only become really high when there is more than one spare available. Advantage can be taken of the high availability of a multiprocessor system, however, if some processor tasks are regarded as dispensible during the rare situations of multiple failures. Examples are the logging of less important process variables, event recording, report generation, etc.

To take full advantage of a multiprocessor configuration, all of the essential functions such as display, direct digital control, and event recording should be grouped into one multiprocessor configuration. This allows all of the computing power to be used in performing essential tasks during an emergency, and at the same time, reduces the amount of spare capacity required. Fig. 9 shows a configuration which is near optimal, within the range of configurations available. 96 K words of store are provided, divided into four blocks, one of which is regarded as spare. The remaining 72 K provides for the basic process control store requirement, plus display and event scan programs. Four processors allow one to be devoted to control, one to display, and one to event scanning, at any time, with one spare.

The unavailability of such a configuration is determined by the disc stores, if these are essential to operation, 0.01% with a capitalized value of $ 5,000. If dependence on disc store is avoided, then the unavailability is determined largely by the main store availability, and is approximately 0.001%, with a capitalized value of $ 500. If an approach is taken which allow less important tasks to be shed, then periods of unavailability are unlikely during the lifetime of the system.

The good availability characteristics of a multiprocessor system bring some disadvantages, however. One is that the failure rate for such a system is high, and good restart facilities are needed for switching between processors, if the very high availability levels are to be achieved in practice. Another problem is that very good protection mechanisms are required between hardware and software components, if they are not to damage each other. The result of such damage is to require extra 'cold restarts' of the system, taking some few minutes. But the effects could be annoying to operators. Multiprocessor system software in general requires much more careful design with respect to interprogram protection, and error recovery, than for single or dual computer systems.

Recovery from store failure in a multiprocessor system cannot be so fast as for a parallel execution dual system, since programs must be reloaded. To allow reliable reload of programs, two cheap disc (floppy disc) or casette tape stores may be provided.

The store multiplexers (multiport units) in a multiprocessor system are relatively expensive. Some saving in cost can be achieved by using a configuration such as Fig. 10, but with some additional costs in software complexity. The cost of the system overall is approximately $ 167,000.

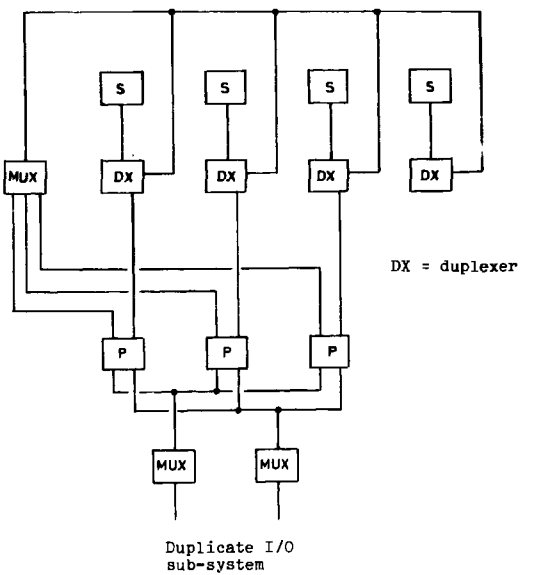


Fig. 10. Reduced multiprocessor system.

	Dual system (1)	Dual system (2)	Multiprocessor	Distributed systems Fig. 17(a)	Fig. 17(b)
Processor $ 6 K	(2) $ 12 K	(2) $ 12 K	(4) $ 24 K	(4) $ 24 K	(6) $ 36 K
Store 4 K = $ 2 K	(96 K) 48 K	(48 K) 24 K	(96 K) 48 K	(4x24K)48 K	(4x8 K) 16 K (2x16K) 16 K
1 disc $ 10 K	10 K	20 K	10 K	(2 x 2)40 K	20 K
Event recording	30 K	30 K	20 K	20 K	20 K
2 floppy discs $ 2 K	2 K	2 K	2 K	4 K	4 K
Switch $ 6 K	6 K	6 K	-	(2) 12 K	(3) 18 K
Multiplexer	(1) 5 K		(4) 20 K	-	
St'd (LP, paper, cassette)	43 K	43 K	43 K	43 K	43 K
	$ 156 K	$ 137 K	$ 167 K	$ 191 K	$ 181 K
Comments	Critical programs in fast store; lowest transient failure rate	disc-based	Critical programs in fast store; performs display processor functions also		

Price comparison
Table 6

Input/Output Subsystem

The input/output subsystem for a 500 MW power plant provides some 1000 analogue channels with an average sampling time of about 1 sec; 2000 digital channels for data logging and on-off control; 30 digital to analogue converter channels for modulating control; 1000 channels for rapid event scanning; and channels for data logging line printers, tape recorders, cassette and paper tape equipment.

The input/output subsystem is one of the most expensive in the overall cost of the computer system. A large part of this cost lies in the signal conditioning equipment which must be devoted to each process data signal line, to change voltage levels, and to provide noise filtering.

A non-redundant system which provides flying capacitor multiplexing and noise filtering on 1000 analogue signal lines costs about $ 80,000. The cost can be reduced and the reliability increased at the same time, by using solid state multiplexing, rather than using reed relays. But problems of common mode noise are increased. The cost of analogue to digital conversion and multiplexing is generally between $ 40 and $ 80 per line. The 30 digital to analogue converters cost about $ 8,000. The cost of on/off inputs and outputs is also high, due to the need for isolation, for achieving a high enough signal level for relay operation, and for providing the correct contact characteristics in the case of power failure (latching, open-on-fail, close-on-fail). For 2000 lines, the cost is about $ 75,000. For alarm monitoring inputs, the cost can be reduced by using matrix multiplexers, but reliability is lower.

The failure characteristics of a computer input/output system are different from the failure of analogue signal transmitters, receivers, and cabling. Fig. 11 shows the general configuration of a large multiplexer input subsystem. Failure of an individual component in such a system can affect many input lines. The most frequent failures occur in the signal conditioning components, since these are the most numerous, and include electromechanical relays. Such a failure affects only one signal line, but repair may affect several signal lines.

Reducing the degree of multiplexing in each unit, before

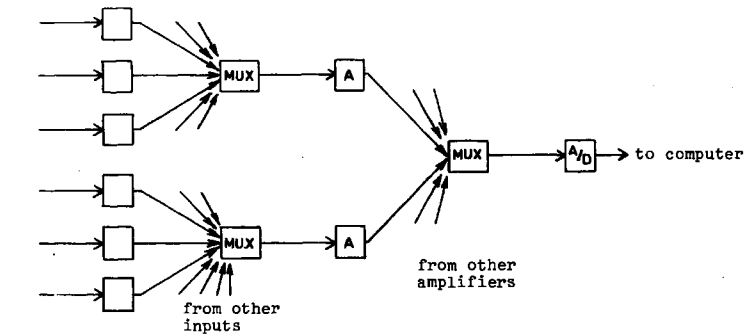


Fig. 11. General form for analogue data acquistion.

reaching the processor, reduces the chance of many signals being affected simultaneously, and reduces the repair problems. Using a larger number of units with a smaller number of lines can also save costs, under modern price conditions. But the failure rate for the input/output system is still high, with an unavailability for all signal lines, of about 1%. Some degree of redundancy is required, but full redundancy is expensive.

There are various ways of implementing any required redundancy - the choice requires a careful and thorough analysis at the design stage. For example, in many cases, the choice of process inputs is far from systematic but instead is based on tradition, cost, vendor requirements, etc. Before one begins to consider redundancy, factors such as the use and usefulness of each I/O point, its criticalness, its relation to other parameters, the possibilities for computer detection and compensation in case of failure, etc. must be taken into account since they play an important role in establishing the required back-up.

Actual forms for redundancy in process I/O include the following:

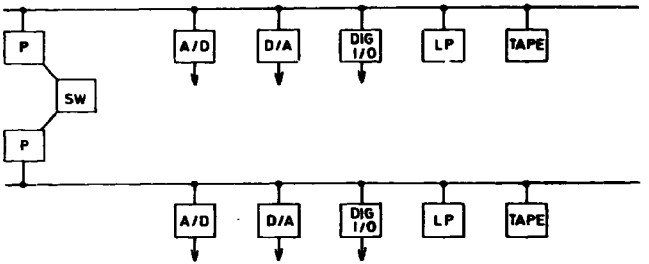
- complete duplication
- use of an m-out-of-n strategy
- employment of diversity - for example
  a) coupling of the same I/O point via several paths
  b) use of alternate data
  c) use of relevant functional relationships.

Reference (2) expands on the use of the computer in improving plant integrity.

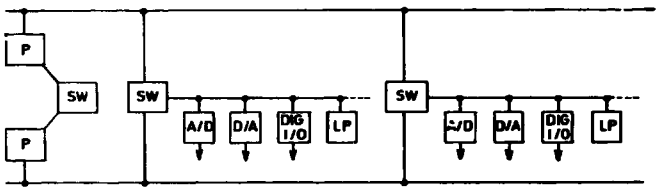
Most analogue data gathering subsystems today are based on the configuration shown in Fig. 11. Alternatives for achieving high-reliability are shown in Figs. 12 and 13. They depend to a large extent on the type of processor redundancy employed.

These alternatives offer in varying degrees the possibilities for

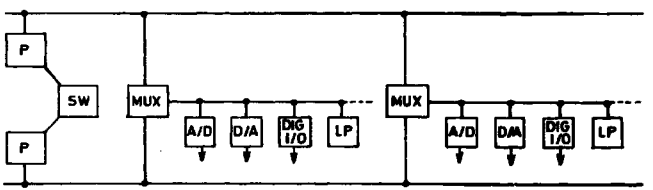
. duplication of analogue and digital input-output - either partial or fully
. sharing of redundant I/O between redundant processors
. distributed multiplexing.



(a) Pure duplicate system, for standby or parallel running redundant processors, duplicate I/O equipment.

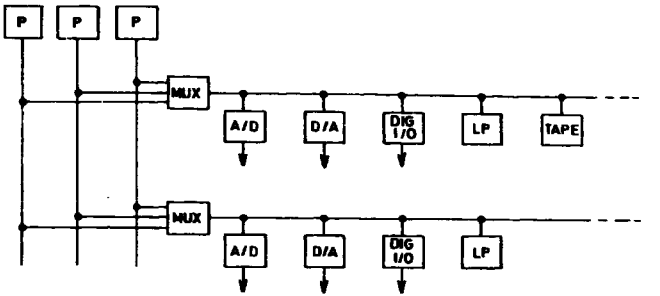


(b) System with transfer switches, for standby redundant processors, duplicate or partially redundant I/O equipment.

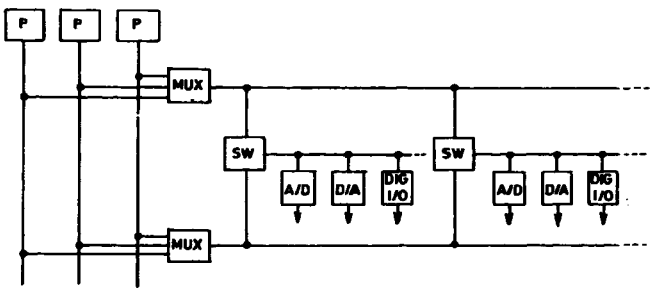


(c) Flexible system with sharable I/O multiplexers, and small separate I/O units, duplicate or partially redundant I/O equipment, for parallel running redundant processors.

Fig. 12. Duplicate processor I/O.



(a) Multiprocessor system with two separate I/O blocks, both fully shareable.



(b) Multiprocessor system with smaller I/O units, partially redundant.

Fig. 13. Multiprocessor I/O.

Two different types of switching are involved for automatic changeover between dual computers; active switching in a standby system, in which the active processor locks out the standby system by periodically renewing the status of the switch; and passive switching in the parallel execution systems (and multiprocessor systems).

Some redundancy of interconnection seems desirable, since it is available relatively cheaply, and offers both reliability and operational advantages.

Systems like the third in Fig. 12, which allow both processors access to all input and output signals continuously by using a multiplexer with two ports, rather than a switch, allow the operator to demand cross checks of instruments and channels, without switching processors. Such capabilities are inherent in the multiprocessor systems. Suitable switches and multiplexers are available commercially.

Most of the remaining equipment for I/O could be duplicated although some, such as magnetic tape, may not require such care. Line printers provide hard copy print out most reliably.

Distributed I/O

A complete alternative to the multiplexing systems described above, is to provide a plant communication system, with analogue to digital converters etc. located local to the instruments and actuators to which they are connected. By using digital transmission over the longer distances, problems of noise are reduced. See (3) for a recent survey and (4) for further details. The savings in cabling cost with this type of system are high. Saving has been quoted as $ 70 per signal line in a refinery in USA. To set against this, remote multiplexing equipment costs about $ 50 per point, or between $ 100 and $ 400 including analogue to digital conversion equipment. The best configurations, with present day prices, depends on the degree of redundancy required for process signals and the current level of wiring costs.

Because of the cyclic nature of the sampling on such systems the response time to alarm inputs can be slow (1/10 sec - 1/4 sec). Some systems allow a limited number of interrupt lines, with a few milliseconds delay at most. But the available communications systems cannot be used for fast event recording, or for

rapid response to alarm or sequential control signals. The total cost of such a system would be about $ 200,000 - $ 300,000 at present day prices, which compares favourably with the costs of $ 160,000 for centralized input/output equipment, and conventional cabling costs (see Fig. 14).

Most of these systems require a small computer to provide sequencing and routing of signals. If the equipment can be integrated into a multiprocessor system. the reliability should be greatly enhanced.

A recent Japanese development (5) represents an additional step forward in this area. This "data highway" system utilizes high speed serial transmission over a double coaxial cable loop with provision for random access to all sensors and actuators as well as interrupt facilities. It is based on the use of low cost LSI devices and furthermore, the method of transformer coupling which is employed between the highway and each station insures a minimum of disturbance to the system in case of station failure. No price data are available at this data (Spring 1973) (see Fig. 15).

In general, there is nothing to prevent the use of a diversified approach which combines various of these types of systems so as to match the varying conditions in the plant as regards sampling, response time, etc. In this way, one could, for example, retain a quick-acting event scanning subsystem in its present form and divide the remaining input-output into appropriate distributed chunks.

Distributed Processing

The computer configurations described earlier provided 'computing power' as a source, in one central block. The availability of mini and micro computers makes it possible to consider more distributed forms of processing, with smaller units dedicated to particular classes of work.

There are two forms that such specialization could reasonably take; according to type of calculation performed; or according to type of equipment controlled.

Retaining minicomputers of the form which are well established today, two configurations are shown in Fig. 16. The advantage of the first configuration is more connected with division

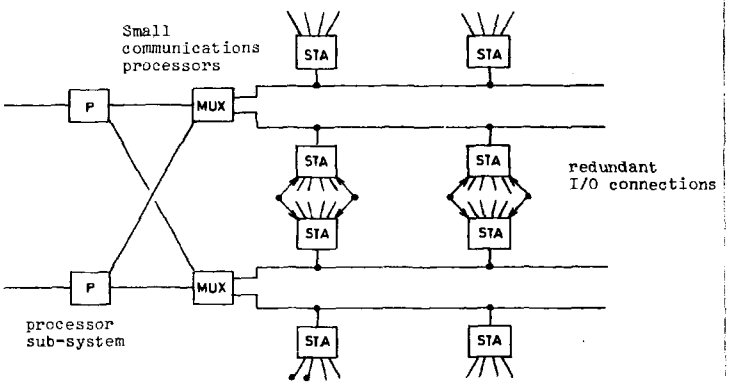


Fig. 14. Plant communication system attached to a dual computer configuration - two sub-systems, each with over 50% capacity, to allow limited redundancy.

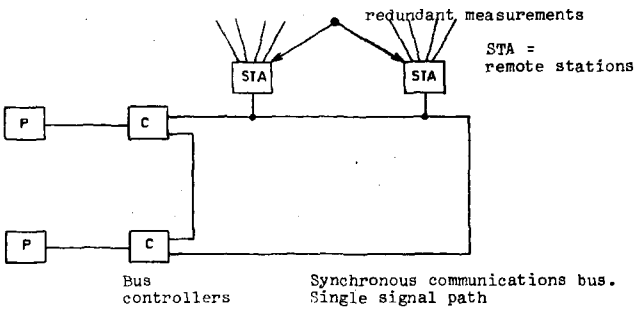
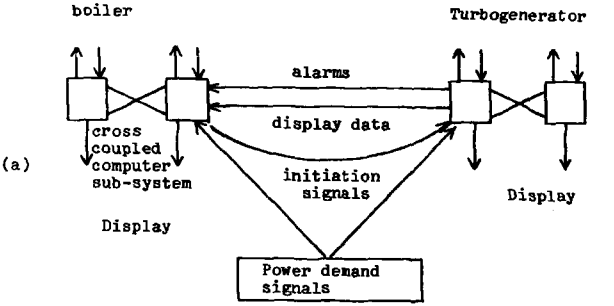


Fig. 15. Communications loop.



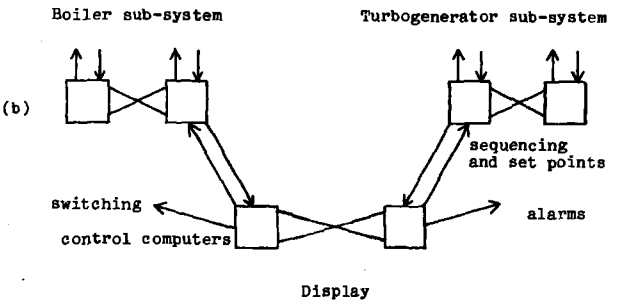


Fig. 16. Distributed processing

responsibility, than with mechanical problems. In many cases, turbogenerator and boiler are supplied by different organisations. It is possible to separate control functions with only a minimal interchange of information between the two subsystems. The boiler control computer is treated as the main computer for display and control purposes since the turbine control logic is more critical, and hence less adaptable. The boiler control computer issues the main power demand and high level sequencing signals to the turbine control computer, and receives responses, data for recording and display and alarm signals in return. Such a system has an additional cost, over that for earlier configurations, because extra processors must be used, and extra store provided for programs for display, and the operating system. Also, if the systems are completely separate, extra disc store must be provided. Dual computers with 24 K of store, and dual discs, could be used for each subsystem, resulting in an additional cost of some $ 50,000.

Fig. 16(b) shows a central control computer, devoted to data logging and display with some additional switching and high level control functions. Two direct digital control subsystems are provided, one for the boiler and one for the turbogenerator. The advantage is that only a limited amount of software and hardware are used in the direct digital control subsystems, improving reliability. The direct digital control components still need to be duplicated, however, for reliability. The direct digital control computers need between 4 and 8 K words of store, of which a large part is for process data. Also, some local store, for program loading, is desirable on the direct digital control computers, perhaps provided by a 'floppy disc' store. The additional cost of this equipment should be about $ 30,000, over the cost of a central dual computer system. The falling cost of minicomputers should have a considerable effect on this figure however. The availability of small, cheap, bulk memories such as bubble memory, should also help to make a configuration of this sort more attractive.

A system like the processor system of Fig. 16(b) would have a very high availability, as far as normal control was concerned. The remote stations for boiler and turbine control are small, and hence have a high hardware availability. And by separating off the immediate digital control programs, the chances of software failure are reduced.

Looking further into the future, systems with a higher degree of distribution should be possible. Development along two different lines is likely arising out of present day growth in desk calculator capabilities, in cheap, 'stripped down' computers for automating mass produced goods such as machine tools, and in the development of digital 'three term' controllers. For control system applications, all of these developments will depend on improvements in plant communication systems.

One form for a distributed control system can be seen in the modern 'energy balance' control systems, which incorporate a large number of feed forward interconnections to individual actuator controllers. Fig. 17 shows the structure of such a system. 'Functional group controllers', one for each of the major controlled variables, serve for local adjustment of actuators, in response to signals from a 'load demand' computer. The local controllers are responsible for starting and adjusting equipment in response to system state signals, and for different levels of load demand.

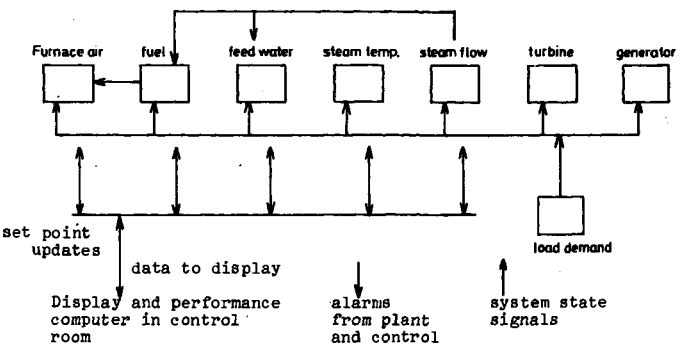


Fig. 17. Functionally distributed control system.

Display of data, and calculation of tuning and performance, are carried out by a control room computer.

The hardware for such a scheme might consist of standard computers intended primarily for the desk calculator market. These are cheap, easily programmed, and already used in data logging applications. Currently, these cost about $ 6,000 each and duplication would be required to provide adequate reliability, but on this basis, the cost is comparable with other duplicate systems such as that of Fig. 7. More important, the cost of this type of computer is likely to drop more dramatically, because of mass production than for other computer types. At the moment, software for control applications is not available, and the computers are somewhat underpowered. But the promise is good.

Development in digital 'process controllers' and 'programmed sequential controllers' is likely to lead in the same direction, but result in still smaller units, connected together via a data bus system. These would then be arranged in 'functional groups'. The direct application of conventional control system design techniques and elimination of programming should make systems of this kind attractive in some applications, and then will benefit from large scale production for smaller control systems.

An alternative to duplication of equipment in such systems, will be apparatus to detect unit failure, coupled with other equipment providing safety control, or switching to manual control. See Fig. 18 for an example. The feature of computer failure which, with proper design, leads to lack of output, makes this approach attractive, since failure in the 'safety' computer will not lead directly to plant failures. Additionally, further conventional safety equipment can be integrated into the scheme.

The biggest advantage of a distributed control system is the hardware isolation between different control functions. This means that the possibility of unwanted interactions in failure situations is very much reduced.

All of the distributed instrumentation systems will depend on a good system of digital interconnection, to reduce noise problems and costs. The presently available plant communication systems are inadequate, because of low data capacity for transmission of rapid event data, and the difficulty of including inter-

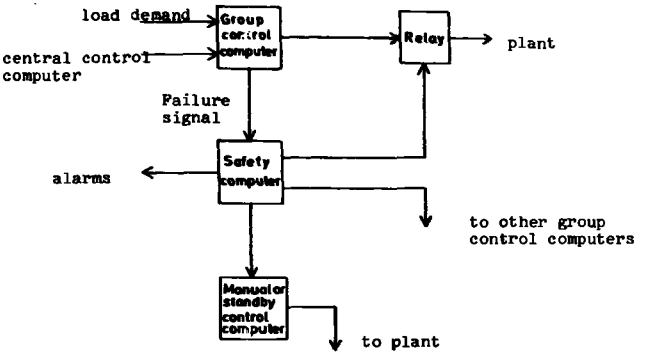


Fig. 18. Instrumentation failure detection and standby control.

rupt signals. Loop systems, which provide 'moving communication slots', to be seized by a transmitting station in a similar way to a passing railway train carriage, have been developed for computer interconnection at Bell Telephone Laboratories (6). Each message is sent to its appropriate address, or broadcast messages can be transmitted.

In such a 'data train' system, local stations are responsible for buffering messages, and retransmitting them to the next station if the address of the data is unrecognized. Protection against failure can be provided, for example, by using a configuration where each station is responsible for checking the correct functioning of the next station, for signalling failure, and for bypassing the station until repair is completed. A system using 2 M bit/sec communication channels should be capable of transmitting up to 10,000 16 bit messages per second around a complete loop, or even more signals between closer points. Costs should be comparable with other plant communication systems, but the delay in accepting interrupt signals should be much lower than for cyclic sampling used in present multiplexing systems.

A communication bus such as the one described here could do more than simply interface controllers and a control processor. It could serve for communication to displays, and for program interchange. Special programming support would be required, to simplify the construction of a system of this sort. An ideal would be to provide software by 'drawing' the equivalent conventional control circuitry, and the display layout, on the screen of an interactive display. Such a system would have a minimum of interaction effects between software units, and allow considerable redundancy both of equipment and control methods. The major cost for redundant components would be for additional analogue to digital conversion channels. A typical example is shown in Fig. 19.

There are two basic modes of using such a communication system - either with the analogue input and output components connected directly to the bus, or with them connected to small minicomputers. The ideal is for the analogue connection to the communication bus to depend on as little hardware as possible, in order to reduce the probability of failure. However, some data reduction and filtering is necessary close to the analogue to digital conversion equipment, to reduce the amount of data transmitted on the bus.

Software

Standard software, for data logging and for 'three term' algorithms for direct digital control, for limit alarm reporting, and for manual control, can be purchased. A major area of weakness at present is in display software. For power plant control, also, many control loops require special non-linear algorithms. Performance evaluation and sequential control software must be supplied anew for each project. Purchasing software can create problems, in that engineering staff do not gain experience with programming.

If only one plant is to be instrumented, the cost of software can be very high. 10 man years would not be an unreasonable estimate for the software production time, starting from scratch, for the basic display plus control software. Development of special training software, such as simulators, and aids to programming such as sequential control languages, would add to this time.

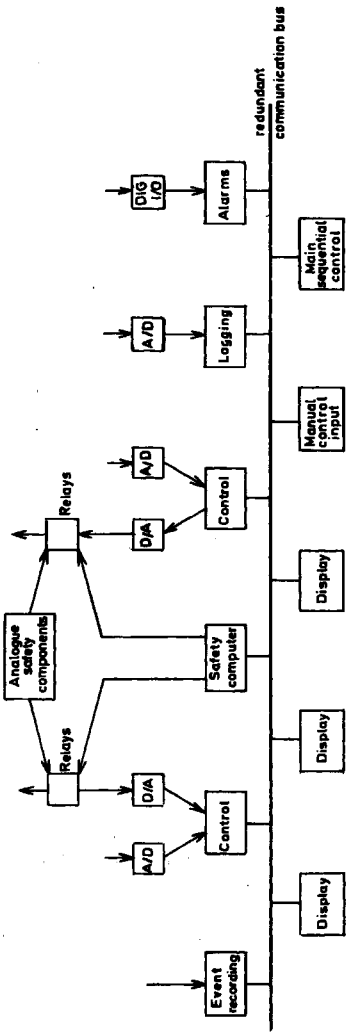


Fig. 19. Distributed system - General types of unit.

The costs can thus be much higher than for design, layout and wiring of a conventional control system. However, most of these costs need not recur, if a software production team is kept together, and programs are reused on several plants. To facilitate this, either the same programming language or the same computer, should be used on a series of installations.

To avoid the risks involved in developing new software after the system has been accepted for use, the ideal is to provide a separate system for programming and testing. The cost of this is justified if the system is small, and used for programming for several installations; or if the programming system is also used for staff training. Such a system should cost about $ 40,000 with display facilities. Alternatively, the standby computer in a dual configuration could be used. Simulation testing before plant commissioning is essential, if no analogue control equipment is provided. Otherwise, commissioning can be seriously delayed.

Estimation of software reliability is difficult, due to the absence of data. But if there is one error per 1000 words of program, the failure rate should be about one failure per three hours, due to simple, non-time dependent failures alone. Removal of such simple failures must be virtually 'complete' (one per 50,000 words) before performance becomes acceptable. In this situation, division of programs into separate 'tasks', and the use of addressing registers with address range limiting, is important to reduce the consequences of a failure.

One form of software for a direct digital control system with sequential control functions is shown in Fig. 20.

Some redundancy in software is one way of avoiding problems with software failures. For example, different routines can be used to provide a direct display channel, and separate programs for actuator operation, when controlling plant manually. To allow this, actuator operation signals should be incremental, so that two controllers can work in parallel if necessary, and it should be possible to shutdown control tasks manually, so that their effect ceases.

When using a duplicate system, every effort should be made to keep copies of programs in the two halves of the system separate, so that an error in one half of the system does not corrupt the other half.

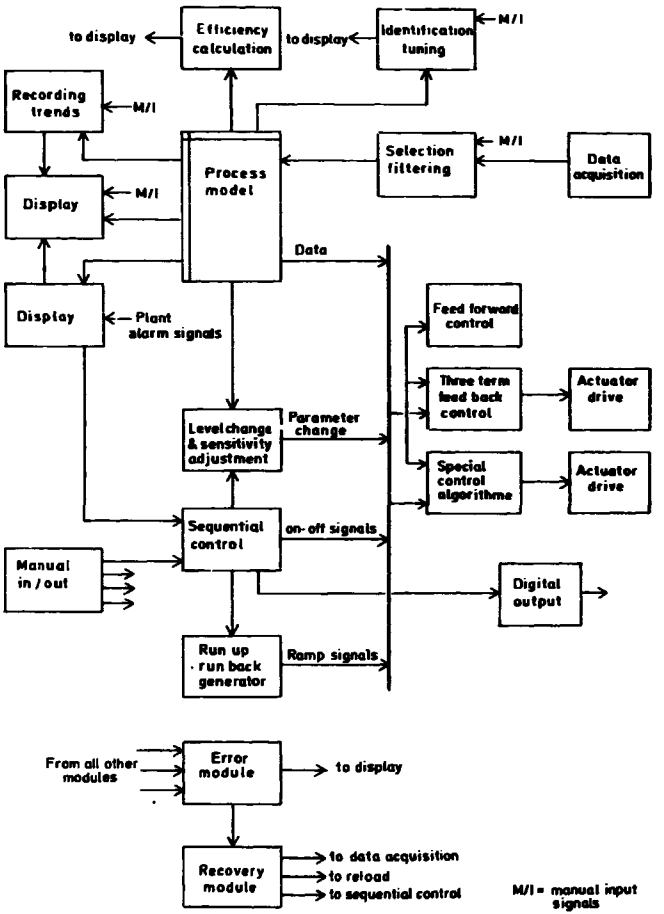


Fig. 20. General form of data flow in direct digital control software.

References - Section IV

(1) Kraftværkskontrol - Økonomisk vurdering af kraftværksautomatisering. DEFU 9/7/70.

(2) "The Improvement of Plant Integrity Using a Process Control Computer". F.P. Lees. Measurement and Control 8/72.

(3) "Line Sharing Systems". R.L. Aronson. Control Engineering 1/71.

(4) "Multiplex Systems Save Multibucks ...". H. Simon. ISA '70 Conference - paper 70-510.

(5) "A Data Highway System". F. Inose et al. Instrumentation Technology. 1/71.

(6) Bell System Technical Journal 6/72.

(7) "Economic Justification of Computer Control Systems". T.M. Stort - Automatica vol. 9, 1973, pp. 9-19.

SECTION V

Conclusions

The descriptions given here have assumed that computer control systems will be used in preference to analogue systems. The use of computers in display and in sequential control functions is reasonably easy to justify on the basis of improved interface to the operator. But, as the cost and reliability figures given earlier show the cost for analogue and direct digital control are comparable. Savings in cabling costs by using plant communications systems may be a deciding factor. The cost of the cheapest configuration with a completely duplicated computer is approximately $ 450,000 or $ 500,000 including a digital communications system to reduce cabling costs.

As was shown earlier, a dual processor system with two discs is most effective, if attention is paid only to availability. A system in which most of the control functions are based in main storage, and with only one disc, may be well worthwhile if the problems of intermittent, rapidly recovered, failures are considered.

A partially redundant, dual, input/output system, consisting of several independent multiplexers, appears as the best configuration among those considered. Ability for both computers to access input data by sharing the multiplexers, gives advantages in rapid switching after failure.

Multiprocessor configurations appear to give no special advantage over dual systems, for power plant use. The very high availability that they offer is not required on economic grounds, so there is no reason to invest in a large amount of software development. However, if an acceptable configuration is available with good software and good intertask protection, there is no technical reason why it should not be used.

Systems in which the DDC functions are separated from sequential control, recording, and display, are likely to show advantages from the point of view of software reliability. The responsibility for different parts of the control system can also be divided in this way. The additional cost is between 5% and 10% of the system price, at present.

Developments in computer system equipment will have a large effect in changing this pattern. Firstly, store costs are falling rapidly, and will continue to do so, perhaps by a factor of four over the next five years. This will reduce the cost by about $ 50,000. (Further reductions in cost have little effect on costs of control, but make more extensive use of the computers attractive).

Secondly, introduction of solid state bulk memories such as 'bubble memory' should make storage of programs and recording much more reliable. The effective cost reduction is not large.

Thirdly, small computers should become available, with a fairly steady cost of about $ 6,000, with 8 K of store, within the next three years, and with steadily improving performance. The choice between these, and much cheaper desk top calculator types of computer, will need to be made at some stage within the next five years. It should be possible to use these computers in distributed systems, in order to reduce the effects of failure. At this stage, it should be possible to provide 'diverse' redundancy, such as separate manual control computers, rather than relying on duplication.

Fourthly, the introduction of plasma, or liquid crystal displays, should reduce costs, increase display definition, and allow increased display sizes. The effect of cost reduction here could well be significant, reducing the cost of the system by some $ 50,000 over the next five years, or perhaps by a larger factor, if these devices become useful for television or teaching purposes.

The area where the largest improvement should be sought in a computer control system, is in plant data input and output and interconnection. With increasing use of LSI, the costs here should fall naturally, but not to as large an extent as store costs, for example.

A major advance in software techniques should be forthcoming within the next two years, that is, a standardized process control version of FORTRAN, with standardized operating system calls. The effect of operating system standardization should extend far beyond FORTRAN programming alone.

The cost of computer control in a power plant, with a high degree of redundancy, is seen to be comparable with analogue instrumentation, provided that software problems and costs are not too great. The actual comparison depends on some detailed costing, and on the prospect for savings in cabling costs.

If good process control software is not available, the cost comparison can be upset, both because of project time and software costs. Two approaches to solution are to buy 'packaged' software or to produce the software 'in house'. Packaged software for process control is available, but the choice of hardware is then constrained, and the commercially available display software is limited. 'In house' development of software means that staff are available to cope with problems after commissioning. But this kind of development is only economic if a degree of continuity can be maintained, both in the production team and design, over several projects.

Developments in computer hardware will be relevant over the next five years, and should lead to reduced system costs and increased reliability. Distributed systems should result in fewer software reliability problems.

Weak areas in the current pattern of commercial development are in display software design; in development of adequate processor and sensor interfacing techniques; in the development of reliable software; and in reducing the costs of interface hardware.

If extensive use is to be made of computerized control systems, then it is very desirable that the image of the computer which is available to the operator should be improved. At the moment, it is manually difficult in the case of failure, to locate which unit has failed. Effective presentation of failure data to operators, coupled with effective techniques for 'switching off' both hardware and software components, should greatly improve the ease with which a diversity of control methods can be used.